A Study of Password Security Factors among Bangladeshi Government Websites

Adil Ahmed Chowdhury, Farida Chowdhury, Md. Sadek Ferdous
Department of Computer Science & Engineering, Shahjalal University of Science & Technology, Sylhet, Bangladesh
Email: adil.aj95@gmail.com, farida-cse@sust.edu, sadek-cse@sust.edu

***Abstract*—The Government of Bangladesh is aggressively transforming its public service landscape by transforming public services into online services via a number of websites. The motivation is that this would be a catalyst for a transformative change in every aspect of citizen life. Some web services must be protected from any unauthorised usages and passwords remain the most widely used credential mechanism for this purpose. However, if passwords are not adopted properly, they can be a cause for security breach. That is why it is important to study different aspects of password security on different websites. In this paper, we present a study of password security among 36 different Bangladeshi government websites against six carefully-chosen password security heuristics. This study is the first of its kind in this domain and offers interesting insights. For example, many websites have not adopted proper security measures with respect to security. There is no password construction guideline adopted by many websites, thus creating a barrier for users to select a strong password. Some of them allow supposedly weak passwords and still do not utilise a secure HTTPS channel to transmit information over the Internet.**

***Index Terms*—Password, Security, Password guidelines, CAPTCHA, Bangladeshi government websites**

I. Introduction

With almost a ubiquitous presence of the Internet, more and more services are provided online using web. A plethora of different web services have had a positive impact on almost every aspect of our human lives. Online services exhibit a number of additional advantages in comparison to the traditional mode of service delivery such as a global 24/7 access, cost savings, ease of use and flexibility, thus narrowing down the gap of accessibility hindrance [1].

Governments from all over the world are also offering an increasing amount of governmental public services via online, the so-called *e-Government* initiative. With the *Digital Bangladesh* initiative, the Government of Bangladesh has pledged to leverage ICTs (Information & Communication Technologies) to facilitate a transformative change in every aspect of the life of a Bangladeshi citizen [2]. Towards this goal, the Government of Bangladesh is offering an increasing number of online public service.

In recent times, different Bangladesh institutions and organisations are facing continuous cyber threats. The Bangladesh Bank Cyber Heist still remains the largest example, in terms of financial loss, of an online security breach for any organisation in the world [3]. Therefore, to counteract these security threats, we must guarantee the security of the offered public services. Indeed, many of these services handle sensitive information and hence, must ensure a restrictive access so that only authenticated and authorised users can access the correct personalised service. To enable this, every user must register at first and then login using an identifier (e.g. username, email address and so on) and a credential. There are a different forms of credentials utilised in online services, however, passwords remain the most widely used one. A recent study estimates that the number of passwords utilised for online services will be around 300 billion by 2020 [4]. Unfortunately, even with its ubiquitous utilisation, password remains one of the major sources of security breaches for online services [5]. That is why it is essential to study and understand different aspects of password security on different Bangladeshi government websites. Surprisingly, there is a pressing gap in this domain. In this paper, we report a study that aims to fill in this gap.

We have conducted a study analysing 36 Bangladeshi government websites and their offered services against six chosen heuristics: password construction guidelines, password recovery mechanism, utilisation of CAPTCHA, security questions, utilisation of HTTPS and password strength meter. Using these six heuristics we aim to gauge the security status and preparedness of Bangladeshi government agencies and suggest a set of recommendations for any weakness found.

Structure: The rest of the paper is structured as follows. Section II describes related work whereas Section III provides a brief background on password authentication along with a discussion of the chosen heuristics for the study. In Section IV, we explain our methodology. Section V presents the results of this study along with their implications and outlines a set of recommendations. Finally, we conclude in Section VI with a hint of future work.

II. Related Work

In this section, we explore a few related researches involving different aspects of passwords and other Bangladesh-focused security studies. Password research has been a widely studied research domain for around three decades or so with a number of influential researches. For example, a review of different types of passwords, their security mechanisms, possible attack methods and weaknesses as well as the password reuse issue can be found in [6]–[9]. There have been a number of researches exploring the influence of culture between different password aspects, such as on the memorability, utilisation and management, and the citizens of different countries [10]–[12].

978-0-7381-2333-2/20/$31.00 ©2020 IEEE

Despite passwords being a widely studied research domain in the field of security, the number of research papers in this domain targeting Bangladeshi citizens and web services are rare. Khan et. al presented a study on Bangladeshi people's knowledge and security awareness about different security practices on the Internet [13]. They took a survey of 1682 Bangladeshi online users and asked them about different security practices like how often they changed their passwords, whether they wrote down or shared their passwords with others and so on. The result was then compared with the users of developed countries and unsurprisingly, they found security knowledge gaps among Bangladeshi users. In a similar study, authors in [14] presented a comparative study of password construction and management strategies between the users of Bangladesh and developed countries. This study also reported that the most of the Bangladeshi users did not follow the general practices to make a password secure. Moniruzzaman et. al examined a number of vulnerabilities in different Bangladeshi websites [15] and found out that many Bangladeshi websites, mostly Bangladeshi government websites, were vulnerable against a number of attack vectors.

These research works explored website securities, password awareness and security practices. However, to the best of the authors knowledge, there is no study exploring the utilisation of different password-related security factors among the government websites of Bangladesh. Such study would be extremely useful to gauge the security status and preparedness of Bangladeshi government agencies. In this paper, we aim to fill in this gap.

III. Password Authentication

To provide personalised online services, the identity of every user must be verified using an authentication mechanism, a process of determining someone's identity [16]. This is an essential mechanism in many real life scenarios when someone has to show an *ID card* to prove their identities to access a service, e.g. borrowing a book from a library. However, authentication becomes indispensable in online services as there is no physical way to prove someone's identity. There are different authentications mechanisms which can be grouped in three different categories [16]: something a user has (like a card or a key), something a user knows (like a secret phrase) and something the user is (bio-metrics such as a fingerprint).

A password is an authentication mechanism that falls under the "the something a user knows" category. It is essentially a shared secret between the user and a service provider relying on the premise that this secret is not shared/disclosed to any other party and this is by which a user can be determined to access personalised services from a web service. There are a number of widely used authentication mechanisms for online services and mobile devices using passwords, bio-metrics such as fingerprints [17], voice [18] and retina [19]. However, password still remains the mostly used and deployed authentication mechanism as other techniques are relatively expensive to implement and maintain.

The security of a password is of paramount importance. If a password is not secure, a user may face a number of security breaches such as the respective account being hacked, data theft and so on [20]. To make a password secure, researchers have devised a number of techniques and guidelines. It has also been found that many users often write down their passwords in papers as they forget them frequently [21]. However, writing down a password is a bad habit as it may compromise the security of the system even if a strong secure password is used. Sharing passwords with friends and families is another bad habit found among general users [22] which a user should avoid doing. Users engage in such activities because of their of lack of knowledge on the importance of password security. Another important factor is how a password is transmitted from the web browser of a user to the service provider during the registration and login phases. Based on the above discussions, we have identified six crucial heuristics, presented below, which are important to assess different aspects of password security for any online service, including Bangladeshi government websites.

- **H1:** Password Construction Guidelines
- **H2:** Password Recovery
- **H3:** CAPTCHA
- **H4:** Security Question
- **H5:** HTTPS Channel
- **H6:** Password Strength Meter

Next, we present a brief discussion of these heuristics.

A. H1: Password Construction Guidelines

There are a number of ways by which a secure and strong password can be constructed. These mechanisms are often outlined in a series of of requirements and recommendations known as *password guidelines* [23]. Depending on the security requirements, different organisations utilise different password guidelines. For example, a password guideline could dictate the length of the chosen password or how different characters such as a small letter, capital letter, digits, or a special character can be mixed together to build a security password. The security of a password is often measured using *entropy* which implies the difficulty of breaking a password using different attack methods such as guessing, brute-force, dictionary attacks and so on [24]. Next, we explore different password constructions guidelines.

A password with at least a length of 8 characters with no composition (construction) requirement, is called *Basic8 composition* [25] and its entropy value is 18 bits. A password with length at least 16 characters with no composition requirement, is called *Basic16 composition* [25] which has an entropy of 30 bits. Another composition requirement titled *Dictionary8* requires a password to of at least length 8 with no dictionary words allowed. Its entropy value is 24 bits. A composition technique with entropy 30 bits where the length requirement is at least 8 does not allow users to use dictionary words and is constructed using upper-case, lower-case, digits, and special characters. This composition is called *Comprehensive8* which has a similar entropy of *Basic16*. A password with a higher entropy is considered more secure.

Displaying a password construction guideline on the website of the service providers during the registration phase (where a user chooses a password) can aid the users to choose a secure password and its enforcement ensures every password meets the minimum security requirements. Such a guideline also indicates the seriousness of the service provider with respect to the security.

B. H2: Password Recovery

Since users need to maintain a number of passwords for many different websites, it is not surprising that they often forget their passwords. In fact, forgetting password is a common issue. To remedy this situation, service providers must provide a password recovery option. There are a number of ways this recovery mechanism can be initiated, e.g. by sending a reset link to the registered email or phone number or via another secure channel.

C. H3: CAPTCHA

A CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a security measure which is used to distinguish between a human and a computer program [26]. A CAPTCHA is designed in such a way that a person can pass the CAPTCHA test which requires to take decisions in a contoured or fuzzy environments. However, a computer program or script fails the test. CAPTCHA is integrated in the registration as well as password recovery phase of a web service to ensure that only valid users are registered to access their services, so as to guard against automated bots utilised by attackers [27]. A CAPTCHA can be of different types such as text, image, audio, video and puzzle, each with their security strengths [28].

D. H4: Security Question

To secure the recovery process, one of the widely used mechanisms is the option of one or more security questions and a user must answer the question(s) correctly before the password recovery option can be initiated. Such a question/answer mechanism can be used to create another layer of security to identify authentic users. Security questions and their answers are recorded during the registration phase and stored in the backend database. Later, when the user wants to recover the password, the chosen security question is asked again to match the answer, thereby cross-checking the authenticity of the user.

E. H5: HTTPS Channel

The service provider also has a crucial role to play for securing a password and other sensitive information while they are transmitted using a web protocol. HTTP (Hypertext Transfer Protocol) is a major web protocol used to transfer data, such as website contents or API calls, over the Internet between a web server and a client such as a browser, a mobile app or another web service. Unfortunately, HTTP is an insecure protocol [29] meaning that every information is transmitted over an HTTP channel in plain-texts. This enables an attacker to observe the network traffic and get hold of sensitive information (such as passwords) transmitted over HTTP. To address this problem, a secure web protocol called *HTTPS* (Hypertext Transfer Protocol Secure) has been devised. HTTPS is a secure extension of HTTP creating an encrypted channel using TLS/SSL on top of HTTP, thereby ensuring the confidentiality, integrity and authenticity of the web server as well as the contents transmitted between the web server and the client. Every web service should utilise the HTTPS channel to ensure that passwords and other sensitive information are never transmitted over an insecure (HTTP) channel.

F. Password Strength Meter

One of the main reasons behind password hacking is the use of a weak password. Because of the lack of knowledge on security, a user may not be aware that (s)he is choosing a weak password. If a visual feedback could be provided when a password is created (during the registration phase), it would help the user to construct a strong password. A password strength meter is a visual representation of the strength of newly created password [30] providing a visual cue, to the user, in real-time. This cue is provided using a combination of text and image where a password strength is categorised by *weak*, *medium* and *strong* texts and a supplementary image reflects this category in different colors. Figure 1 shows a sample of a password strength meter where a red color indicates that the given password is weak whereas green would refer it to be a strong password. It has been argued that a password strength meter can a great aid for the users [31] and that is why it has been included as one of our heuristics.

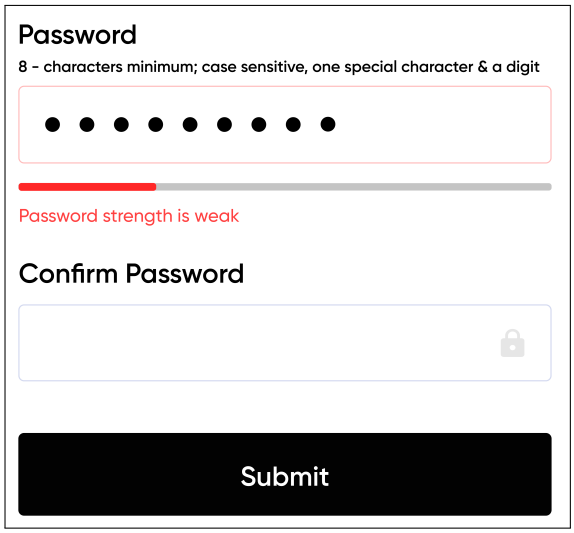

Fig. 1: Password Strength Visualisation

IV. Methodology

The methodology of our study is summarised in Algorithm 1. At first, we have compiled a list of 120 Bangladeshi Government websites (denoted with $govList$ in Algorithm 1) by exploring the National portal of Bangladesh [32] (an integrated online portal recording all websites/services by the Bangladeshi government).

Algorithm 1: Methodology

```
1  Input: govList → all Govt. websites
2  Output: selList → selected websites with observations
3  Start
4      selList = loginFunc(govList);
5      while x ∈ selList do
6          for i ← 1 to 6 do
7              if x satisfies H_i then
8                  selList.H_i = "Yes";
9              else
10                 selList.H_i = "No";
11             end
12         end
13     end
14     function loginFunc(govList)
15         while x ∈ govList do
16             if x has login functionality then
17                 selList = selList ∪ x;
18         end
19         return selList;
```

In the next step, we have shortlisted (denoted with *selList* in Algorithm 1) the *govList* by visiting each website individually one by one and checking if they have any registration and login features so that a user can create an account for getting services from the website. The motivation behind this step is that not all websites will require registration and login features and hence, they do not need to deal with passwords and can be excluded. This process is explained in line 4 and lines 14 to 18 in Algorithm 1. At the end of this step, we have managed to find 36 websites that meet our criteria. Among these 36 websites, the majority (30, around 83%) provide services whereas five (13.8%) provide information and one is a training website. The detailed information regarding these websites along with their URLs and purposes is presented in Table I.

In the final step, we have visited these 36 websites one by one, created an account and investigated if each website satisfies the selected six heuristics as outlined in lines 5 to 12 in Algorithm 1. Consequently, we have marked the heuristic for that respective website with a 'Yes' (line 8 in Algorithm 1). Otherwise the heuristic has been tagged with a 'No' (line 10 in Algorithm 1) with some additional comments.

V. Results & Discussion

In this section, we present and analyse the findings of our study (Section V-A) along with a discussion and a set of recommendations (Section V-B).

A. Analysis

Now, we present an analysis of the findings of our study for each heuristic. Our findings for all heuristics have been summarised in Table I where the symbol "●" has been used (for all heuristics except H1) to denote if a particular website satisfies a respective heuristic or the symbol "○" has been used to denote the opposite (not satisfied) whereas *PS* implies that the password is provided by a website. We have counted the number of heuristics satisfied by each investigated website and the distribution of satisfied heuristics are presented in Figure 2 for H1 and Figure 3 for other heuristics.

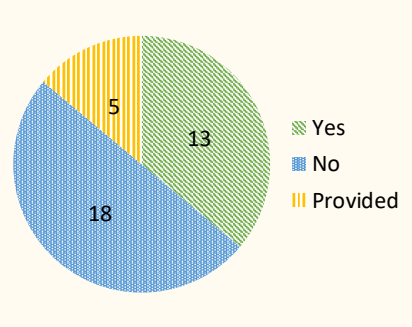

Fig. 2: H1 Distribution

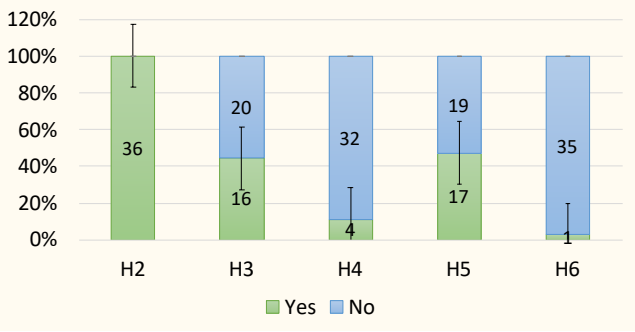

Fig. 3: Satisfied Heuristics in Selected Websites

H1: From the selected websites, 13 websites provide and enforce a password construction guideline (Figure 2). 18 websites do not provide any guidelines and allow a password of any length and strength to be created. On the remaining 5 websites, the password for a user is created by the system which is then supplied to the user. Three out of these five websites utilise an OTP (One Time Password) sent over another channel (e.g. email, mobile phone and so on) during the registration as well login phases instead of using a fixed password. This is an alternative mode of authentication, however, the user might face severe consequences when the user loses control of the registered phone number or email address. Among the 13 websites providing guidelines, they have adopted a wide variety of guidelines. We have grouped these guidelines in seven different categories as presented below, where *PG* stands for *Password Guideline*. Out of these guidelines, PG-6 is supposedly more secure if no dictionary word is used. PG-1 can be the least secure one as it allows a password of only four characters without any mixture of letters, numbers and special characters. Even PG-7 can be vulnerable since it allows any password length.

- **PG-1**: At least 4 characters
- **PG-2**: At least 6 characters

TABLE I: Detailed Information of 36 Websites

Website	URL	Purpose	H1	H2	H3	H4	H5	H6
E challan	http://echallan.gov.bd/login	Online challan service	○	●	●	○	○	○
Travel Agency Management System	https://regtravelagency.gov.bd	Agency registration service	PS	●	○	○	●	○
Police Clearance	http://pcc.police.gov.bd/	Police clearance service	PG-6	●	●	○	○	○
eRecruitment System	https://erecruitment.bcc.gov.bd/exam/users/login	Online Recruitment service	PS	●	●	○	●	○
Bangladesh Investment Development Authority	https://osspid.org/user/create	Investor registration service	PS	●	●	○	●	○
Bangladesh Scouts	http://service.scouts.gov.bd/login	Member registration	○	●	●	○	○	○
eTin	https://secure.incometax.gov.bd/TINHome	eTin registration service	PG-4	●	●	●	●	○
Directorate General of Drug Administration	https://www.dgda.gov.bd/	Drug regulatory authority service	○	●	○	○	●	○
eVeterinary	http://evet.gov.bd/registration	Veterinary information	○	●	○	○	○	○
Dhaka Power Distribution Company Limited	https://dpdc.org.bd/career/	Career portal service	PG-3	●	○	○	●	○
ePayment	http://nbrepayment.gov.bd/	Tax service	PG-1	●	●	●	○	●
NBR - learning	http://nbrelearning.gov.bd/page/sign-up	eLearning information	○	●	○	○	○	○
EkSheba	https://eksheba.gov.bd/	Integrated service portal	PS	●	○	○	●	○
National e-Government Procurement	https://www.eprocure.gov.bd/	Govt. procurement service	PG-6	●	●	●	●	○
Biman Airlines	https://www.biman-airlines.com/member/registration	Online booking service	○	●	○	○	●	○
VAT	https://www.vat.gov.bd/	Tax return service	PS	●	○	●	●	○
Bangladesh Telecommunication Regulatory commision	https://naid.btrc.gov.bd/	IMEI checking & NOC information	○	●	○	○	●	○
Bangladesh Customs	http://103.48.18.166/signup	Auction service	PG-5	●	○	○	○	○
Trade License	http://www.etradelicense.gov.bd/DefaultEng	Trade license service	○	●	○	○	○	○
Passport	http://passport.gov.bd/Application-1.aspx	Passport application service	○	●	○	○	○	○
Teletalk	http://www.teletalk.com.bd/	Telecommunication service	PG-5	●	●	○	○	○
Rajuk	http://cp.rajuk.gov.bd/user/signup	Land/Construction permit	PG-2	●	●	○	○	○
eFire License	http://efirelicense.gov.bd/apply-license-renew	Fire license service	○	●	○	○	○	○
Chief controller of import and export	https://olm.ccie.gov.bd/login	License approval & renewal	○	●	●	○	●	○
Mukhtopaath	http://www.muktopaath.gov.bd/register	e-Learning platform service	PG-4	●	○	○	○	○
BCC-CA	https://www.bcc-ca.gov.bd/	Certifying authority service	PG-7	●	●	○	●	○
Dokkhota Batayon	http://skills.gov.bd/login	Work-placement service	○	●	○	○	●	○
North west power generations company	http://career.nwpgcl.gov.bd/	Online job application service	○	●	○	○	○	○
Skill connect	http://portal.bdskills.gov.bd	Training portal	○	●	○	○	○	○
Bangladesh Road Transport Authority	https://www.ipaybrta.cnsbd.com/index/carowner	Vehicle fees and taxes payment service	PG-4	●	●	○	●	○
Shikkhok batayon	https://www.teachers.gov.bd/	Blog	PG-2	●	○	○	●	○
Agni Nirbapon	http://www.noc.fireservicebd.info/auth/register	Exemption certificate service	○	●	●	○	○	○
BAERA	https://ells.baera.gov.bd/	Nuclear control program authority info.	○	●	●	○	●	○
Bangbandhu Sc. & Tech. Fellowship	http://fellowship.bstft.gov.bd/	Fellowship application service	PG-4	●	○	○	○	○
Bostro Odhidoptor	http://e-application.dot.gov.bd/public/public/home	e-Service for textile department	○	●	○	○	○	○
NID	https://services.nidw.gov.bd/nid-pub/citizen-home/	NID registration, correction service	○	●	●	○	○	○

- **PG-3**: At least 6 characters with a mixture of letters and numbers
- **PG-4**: At least 8 characters
- **PG-5**: At least 8 characters with a mixture of letters and numbers
- **PG-6**: At least 8 characters with a mixture of letters, numbers and special characters
- **PG-7**: A mixture of letters, numbers and special characters with no specified length

The corresponding guideline has been used in the respective field for H1 column in Table I. The distribution of these guidelines among the 13 websites are presented in Figure 4. As per the figure, the mostly adopted guidelines is PG-4 requiring a password length of 8 characters adopted by 4 websites.

H2: Password recovery factor being a basic security mechanism, has been found in all 36 websites (Figure 3). However, the interesting observation is the recovery channel utilised by different websites. For example, 24 websites (more than 66%) have adopted emails as their password recovery channel into which the password reset links are sent. Such links are valid

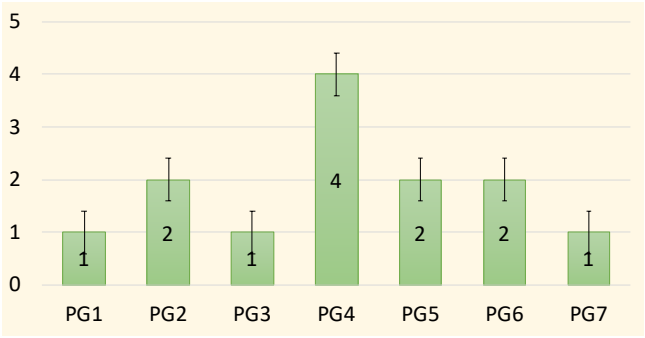

Fig. 4: Distribution of Password Guidelines

for a specific amount of time and passwords must be reset within that validity period. Mobile phones have been adopted as the password recovery channel by 7 website where an OTP is sent to reset the password. The remaining 5 websites use both of these channels for password recovery.

H3: As reported in Table I and Figure 3, CAPTCHA input is mandatory during the registration process on 16 websites while the rest of the 20 websites do not employ any CAPTCHA. As explained earlier, CAPTCHA might guard against the creation of falsified accounts via automated computers programs. Therefore, it is highly recommended to employ CAPTCHA and the websites which do not utilise CAPTCHA are susceptible against such attacks.

H4: As per our investigation only 4 websites (Figure 3) have asked security questions during the registration phase. Examples of some of the questions asked are:

- What is the name of your favourite book?
- What is the name of your first school?
- What is your mother's maiden name?
- What was your dream job as a child?
- Who was your childhood hero?

Other 32 websites has no security question, thus, an attacker can falsely and easily initiate an account recovery process.

H5: It has been a surprise for us to observe that only 17 websites (Figure 3) utilise an HTTPS channel, indicating that they are aware of the importance of a secure protocol. Unfortunately, the other 19 websites rely on the insecure HTTP channel and hence, they remain extremely insecure, and every information, including passwords, transmitted to these websites might be visible to attackers during the transmission.

H6: Another surprising finding is that only one website (Figure 3) provides a password strength meter during the registration phase. Such a visualisation feature helps any user to create a strong and more secure password. That is why it is crucial that any website requiring a password entry should implement a password strength meter.

B. Recommendations

In this section, we present a number of recommendations to improve the security, with respect to passwords, of Bangladeshi government websites.

Recommendation-1: It is imperative that every governmental website adopts and enforces a secure password construction guideline. This will ensure that users do not opt in for easy-to-guess insecure passwords. However, as we have found, there are a wide-range of password guidelines adopted by different governmental websites. To ensure a streamlined approach, we recommend to adopt (and show) a unified password construction guideline by (on) all governmental websites during the registration procedure. In addition to this, a password strength meter should be utilised to aid users selecting a secure, strong and compliant password.

Recommendation-2: Every governmental website must employ secure CAPTCHA mechanisms during the registration as well as password recovery phases. There are a wide-range of CAPTCHAs available varying in their types, security and usability. A unified policy for CAPTCHA should be devised and adopted for all governmental websites.

Recommendation-3: Each governmental website that deals with user registrations including password creation, storage and management must adopt an HTTPS-only policy to secure network traffic to and from their website.

Recommendation-4: The secure storage of passwords is also very crucial. In an ideal scenario, every single password should never be transmitted via the network to the server. Instead, they should be hashed at the user side before their transmission (resp. storage) to (in) the server. This reduces the risk of password leakage in case a breach occurs at the respective server. Alternatively, it must be ensured that passwords are transmitted through an HTTPS channel and stored in encrypted form in the backend database.

Recommendation-5: Needing to create many accounts across different websites, a user will ultimately face the ill consequence of password fatigue [9], a pressing feeling to remember and manage passwords for so many websites. This forces a user to reuse one or two secure passwords for different websites, thereby increasing the chance of attacks [20]. An effective technique to offset password fatigue in the governmental setting is to adopt the notion of an *Identity Federation*. An identity federation is a trusted service model in which different service providers (known as *SPs*) are tied together under a formal agreement with a single identity provider (*IdP*) [33]. The IdP handles all identity activities such as identity creation, storage and management. Users need to register with that single IdP and they can access services from federated SPs using a single credential, thus significantly reducing the probability of password fatigue. Towards this aim, a proposal for a country-wide identity federation for Bangladesh was put forward by the authors in [34]. Sadly, it was difficult to adopt this approach previously as there was no central identity database in Bangladesh. However, with the current National ID database and its associated service such as Porichoy (`https://porichoy.gov.bd/`), Bangladesh currently has the infrastructure to deploy a nation-wide identify federation. We highly recommend to adopt this approach.

VI. Conclusion

In this paper, we have presented a study of password security among 36 different Bangladeshi government websites against six carefully-chosen password security heuristics. The main motivation is to understand the password security status of the chosen websites which in a way acts as the reflection of the password security awareness and preparedness among the corresponding government agencies. Our findings suggest that many websites have not adopted proper security measures. Many of them do not utilise any password construction guideline which can act as a barrier for users to select a strong password. Even the security guidelines employed by a few websites are not so secure. Similarly, many websites still do not leverage the HTTPS capability to securely transmit information, indicating a lack of knowledge as well as preparedness with respect to security. We hope that our study sheds some lights on some important password security factors and the respective authority takes a note of their lacking and act accordingly. However, it must be pointed out that passwords are just a single aspect of the overall security of any website. A rigorous evaluation of the remaining aspects must be carried out to fully understand the comprehensive security status and preparedness of different Bangladeshi government websites which we aim to do in future.

References

[1] B. Queensland. (2016, 13 June) "Benefits of doing business online". Accessed: 07-09-2020. [Online]. Available: https://www.business.qld.gov.au/starting-business/internet-start-ups/online-basics/benefits

[2] A. to Information (A2I) Programme: Prime Minister's Office. (2011, January) Strategic priorities of digital bangladesh. [Accessed: 07-09-2020]. [Online]. Available: https://a2i.gov.bd/wp-content/uploads/2017/11/4-Strategy_Digital_Bangladesh_2011.pdf

[3] K. Zetter. (2016, 17 May) "That Insane, $81M Bangladesh Bank Heist? Here's What We Know". [Online; accessed 07-09-2020]. [Online]. Available: https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/

[4] R. Sobers. (2020, 21 July) 110 must-know cybersecurity statistics for 2020. [Accessed: 07-09-2020]. [Online]. Available: https://www.varonis.com/blog/cybersecurity-statistics/

[5] L. Arezina. (2019, 19 November) Password statistics for 2020. [Accessed: 07-09-2020]. [Online]. Available: https://dataprot.net/statistics/password-statistics/

[6] D. V. Klein, "Foiling the cracker: A survey of, and improvements to, password security," in *Proceedings of the 2nd USENIX Security Workshop*, 1990, pp. 5–14.

[7] M. Raza, M. Iqbal, M. Sharif, and W. Haider, "A survey of password attacks and comparative analysis on methods for secure authentication," *World Applied Sciences Journal*, vol. 19, no. 4, pp. 439–444, 2012.

[8] P. Hoonakker, N. Bornoe, and P. Carayon, "Password authentication from a human factors perspective: Results of a survey among end-users," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 53, no. 6. SAGE Publications Sage CA: Los Angeles, CA, 2009, pp. 459–463.

[9] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, "The tangled web of password reuse." in *NDSS*, vol. 14, no. 2014, 2014, pp. 23–26.

[10] C. Yang, J.-l. Hung, and Z. Lin, "An analysis view on password patterns of chinese internet users," *Nankai Business Review International*, 2013.

[11] A. Constantinides, M. Belk, C. Fidas, and G. Samaras, "On cultural-centered graphical passwords: Leveraging on users' cultural experiences for improving password memorability," in *Proceedings of the 26th Conference on User Modeling, Adaptation and Personalization*, 2018, pp. 245–249.

[12] H. M. Aljahdali and R. Poet, "The affect of familiarity on the usability of recognition-based graphical passwords: Cross cultural study between saudi arabia and the united kingdom," in *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE, 2013, pp. 1528–1534.

[13] R. Khan and R. Hasan, "Security-aware passwords and services usage in developing countries: A case study of bangladesh," in *International Conference on Services Computing*. Springer, 2018, pp. 67–84.

[14] S. T. Haque, T. Alam, M. Al-Rasheed, and M. Wright, "Password construction and management strategies of the online users of bangladesh: A demographic comparison with the users of the first-world countries," in *Workshop on Human and Technology*, 2013.

[15] M. Moniruzzaman, F. Chowdhury, and M. S. Ferdous, "Measuring vulnerabilities of bangladeshi websites," in *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)*. IEEE, 2019, pp. 1–7.

[16] M. T. Goodrich and R. Tamassia, *Introduction to computer security*. Pearson, 2011.

[17] A. R. Roddy and J. D. Stosz, "Fingerprint features-statistical analysis and system performance estimates," *Proceedings of the IEEE*, vol. 85, no. 9, pp. 1390–1421, 1997.

[18] L. Zhang, S. Tan, J. Yang, and Y. Chen, "Voicelive: A phoneme localization based liveness detection for voice authentication on smartphones," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 1080–1091.

[19] C. Mariño, M. G. Penedo, M. Penas, M. J. Carreira, and F. Gonzalez, "Personal authentication using digital retinal images," *Pattern Analysis and Applications*, vol. 9, no. 1, p. 21, 2006.

[20] B. Ives, K. R. Walsh, and H. Schneider, "The domino effect of password reuse," *Communications of the ACM*, vol. 47, no. 4, pp. 75–78, 2004.

[21] R. Morris and K. Thompson, "Password security: A case history," *Communications of the ACM*, vol. 22, no. 11, pp. 594–597, 1979.

[22] R. Shay, S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor, "Encountering stronger password requirements: user attitudes and behaviors," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, 2010, pp. 1–20.

[23] S. Furnell, "An assessment of website password practices," *Computers & Security*, vol. 26, no. 7-8, pp. 445–451, 2007.

[24] W. Ma, J. Campbell, D. Tran, and D. Kleeman, "Password entropy and password quality," in *2010 Fourth International Conference on Network and System Security*. IEEE, 2010, pp. 583–587.

[25] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman, "Of passwords and people: measuring the effect of password-composition policies," in *Proceedings of the sigchi conference on human factors in computing systems*, 2011, pp. 2595–2604.

[26] L. Von Ahn, M. Blum, N. J. Hopper, and J. Langford, "Captcha: Using hard ai problems for security," in *International conference on the theory and applications of cryptographic techniques*, 2003, pp. 294–311.

[27] A. I. Rusu, R. Docimo, and A. Rusu, "Leveraging cognitive factors in securing www with captcha." in *WebApps*, 2010.

[28] V. P. Singh and P. Pal, "Survey of different types of captcha," *International Journal of Computer Science and Information Technologies*, vol. 5, no. 2, pp. 2242–2245, 2014.

[29] E. Rescorla, "RFC2818: HTTP Over TLS," 2000.

[30] B. Ur, P. G. Kelley, S. Komanduri, J. Lee, M. Maass, M. L. Mazurek, T. Passaro, R. Shay, T. Vidas, L. Bauer *et al.*, "How does your password measure up? the effect of strength meters on password creation," in *21st USENIX Security Symposium*, 2012, pp. 65–80.

[31] X. de Carné de Carnavalet and M. Mannan, "From very weak to very strong: Analyzing password-strength meters," in *Network and Distributed System Security Symposium*, 2014.

[32] Bangladesh National Portal. [Accessed: 07-09-2020]. [Online]. Available: https://bangladesh.gov.bd/index.php

[33] D. W. Chadwick, "Federated identity management," in *Foundations of security analysis and design V*. Springer, 2009, pp. 96–120.

[34] M. S. Ferdous, M. J. M. Chowdhury, M. Moniruzzaman, and F. Chowdhury, "Identity federations: A new perspective for bangladesh," in *International Conference on Informatics, Electronics & Vision*, 2012, pp. 219–224.