An Application-centric Survey of Security and Privacy Issues: Bangladesh Perspective

Farida Chowdhury
Computer Science and Engineering
Shahjalal University of Science and Technology
Sylhet, Bangladesh

ABSTRACT

In recent years, we have seen a number of research works reported which target different security and privacy issues in Bangladesh. To understand their scopes, it is essential to have a clear picture of the application domains they have covered and different security and privacy issues they have analysed and identified. In essence, a survey of all major works covering different security and privacy aspects with a specific focus in Bangladesh is required and is still missing. In this paper, we present an application-centric survey covering studies of security and privacy issues in Bangladesh perspective, utilising an application as well as study centric taxonomies. A total number of 19 research papers have been identified and thoroughly reviewed according to the formulated taxonomies. Finally, we present a summary of our analysis using tabular formats, clearly identifying the scopes as well as applications domains for each reviewed work.

General Terms

Security, Privacy

Keywords

Security, Privacy, Password, Survey, Bangladesh

1. INTRODUCTION

The Internet and online based services have become a part and parcel of our day to day lives. There are a wide-range of such services covering a large landscape of application domains touching our lives in almost in every single aspect. However, the impact of such online services is much more evident in developed countries than any developing nation such as Bangladesh. Indeed, Bangladesh has a considerably late exposure to plethora of online services [1]. At the initial stage, the adoption rate of online services in Bangladesh has been quite slow. However, the usage of the Internet and different online services have started to gather momentum in the last decade or so. Currently, there are around 110 Million Internet subscribers in Bangladesh as of October 2020 which is expected grow even more in the future [2].

With the growing usage of the Internet and different online services, sensitive and private personal information is transmitted. The lack of any security measure to safeguard the security and privacy of such information may often lead to disaster for any respective person as well as for the organisation which deals with such information [3, 4]. Therefore, it is of paramount importance to ensure the security and privacy of such information.

Understandably, there have been a wide variety of measures to facilitate this goal. However, it is important to understand the effectiveness of such measures both at the personal level and the organisation level. There have been a number of studies measuring the effectiveness of security [5, 6] and privacy [7, 8]. Unfortunately, the majority of these studies are targeted for developed countries. To ensure a proper and fruitful adoption of the Internet, such studies targeting a developing nation such as Bangladesh is essential. This is because there are a number of differences in cultural factors, gaps in knowledge and technology use in between a developed and developing nation which would dictate how successful a security and privacy measure is successfully adopted in a developing nation [9].

In recent years, we have seen a number of research works reported which target different security and privacy issues in Bangladesh. To understand their scopes, it is essential to have a clear picture of the application domains they covered and different security and privacy issues they analysed and identified. In essence, a survey of all major works covering different security and privacy aspects with a specific focus in Bangladesh is required and is still missing. We aim to fill in this gap with this article. The main contributions of this articles are:

The article presents an application-centric taxonomy and a study-centric taxonomy using which the survey is conducted.

Using the taxonomy, different Bangladesh-focused security and privacy research works have been analysed.

Finally, the survey result is presented in a tabular fashion so as to visualise the comparative analysis of the selected works in a concise way.

The article is organised as follows. In Section 2, we present the survey taxonomy. The security works are reviewed in Section 3 and the privacy works are reviewed in Section 4. We present our survey analysis in Section 5. Finally, Section 6 concludes the article.

2. APPLICATION & STUDY CENTRIC SURVEY TAXONOMY

For the survey, we have utilised two different taxonomies: one for the application and the other for the study.

The application-centric taxonomy, presented in Figure 1, represents the application domain(s) for a specific research work.

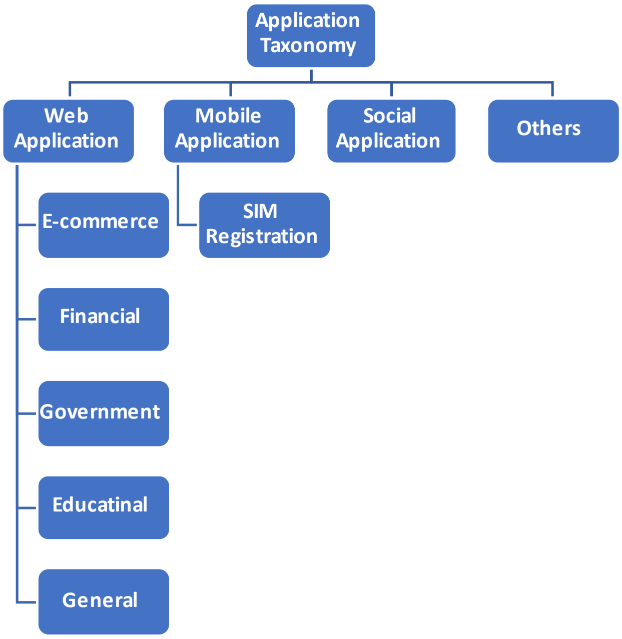

Fig. 1. Taxonomy of Application

We have categorised the application taxonomy in four categories: web application, mobile application, social application and others. A web application most focuses four different types: e-commerce, financial, Government, educational and general. A mobile application exclusively covers SIM registration process. A social application, on the other hand, explores some social phenomenon. The others category represents application domains not covered by the previous three.

The study-centric taxonomy is illustrated in Figure 2. This taxonomy represents the study areas for the selected research works and is divided into two categories: security and privacy. The security study deals with security areas for different research works. There are four major security areas: vulnerability assessment, password, policy and others. The vulnerability assessment area itself has different sub-areas as illustrated in Figure 2. On the other hand, the privacy study deals with five different areas: general privacy, health data privacy, repair centre privacy, service/flexiload centre privacy and phone sharing privacy.

3. REVIEW OF SECURITY WORKS

There are a number of research works focusing on the different security aspects in Bangladesh perspective. In this section we review these works.

Farah et al. studied the possibility of XSS (Cross Site Scripting) and CSRF (Cross-Site Request Forgery) vulnerabilities in 500 Bangladeshi websites [10]. For their study, the utilised a black box testing methodologies where they analysed the HTML source of each website to identify any XSS vulnerability. For identifying CSRF vulnerability, the authors investigated the HTTP request and response for each website as well as submitted suspicious queries to each each website. If the target website accepted any such malicious query, the website is tagged as vulnerable. Their study revealed that 335 websites out of 500 were vulnerable to either XSS or CSRF. Among the vulnerable websites, 25% were vulnerable to XSS, 40% were vulnerable to CSRF and 40% were vulnerable to both of them. One limitation of their study is that they did not provide any details regarding the analysed website types.

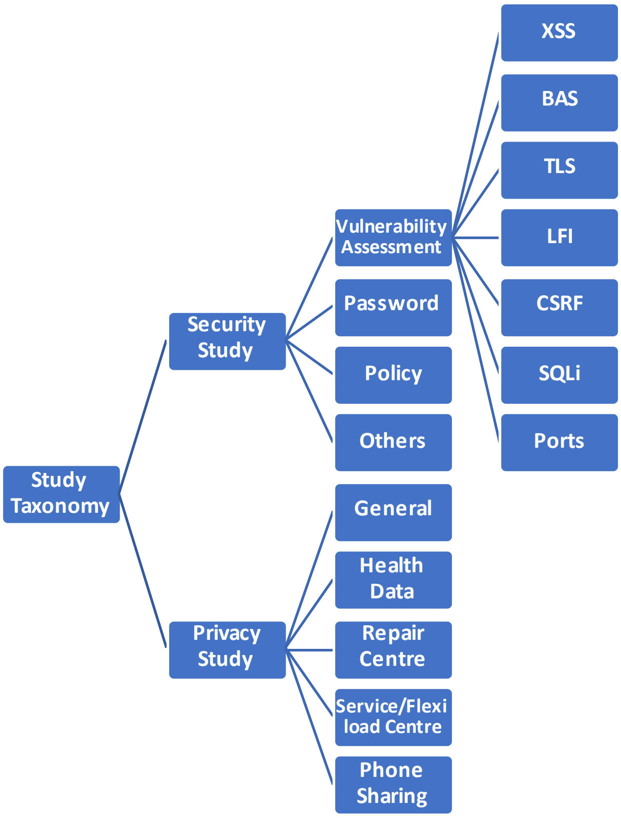

Fig. 2. Taxonomy of Study

In a similar vein, Moniruzzaman et al. evaluated 34 popular websites covering a wide-range of application domains such as government, education, stock exchanges, banking, blogging, news and others [11]. The evaluation was carried out against 6 major security attack vectors:

SQL Injection

XSS and

BAS (Broken Authentication and Session)

CSRF (Cross-Site Request Forgery)

Unusual Ports

TLS (Transport Layer Security)

For each website, different information at first was collected using different tools. Then, both black box and white box testing methods were employed to find vulnerabilities. As per their evaluation, 64% of the selected websites exhibited at least one vulnerabilities with the government websites were less secure. Among the vulnerabilities, 28% of websites had SQL injection vulnerability, 27% had TLS vulnerability, 26% had XSS vulnerability, 10% had BAS vulnerability, 7% had CSRF vulnerability and 2% had other vulnerabilities.

Begum et al. analysed a critical vulnerability called *Local File Inclusion* (LFI) [12]. LFI has several types, however, the authors analysed the following three types in their study:

Generalised LFI

Remote File Inclusion (RFI)

Structured Query Language Injection (SQLi)

The authors adopted a black box approach and selected 153 LFI vulnerable Bangladesh websites. Then, they analysed the websites in details to identify what type of LFI vulnerabilities could be found on these selected websites. As per their analysis, 85 websites were vulnerable to Generalised LFI, 51 websites were vulnerable to SQLi and the rest 17 websites were vulnerable to RFI. The authors also claimed that, out of 153 websites, 77 could be fully compromised, 24 websites could be accessed with admin level privilege, password storage files could be accessed for 33 websites. The limitation of the study is that the author did not explain the methodologies for collecting 153 LFI vulnerable websites. Also, it is not clear how the authors found out if a website could fully compromised or accessed using admin level privilege.

Similarly, Farah et al. analysed 108 financial web applications within a wide range of domains such as banks, e-commerce websites, brokerage houses, insurance companies and educational institutions [13]. To analyse the vulnerabilities, they conducted SQLi (Structured Query Language Injection) penetration testing using the following two methods:

SQLi without evading IDS (Intrusion Detection System)

SQLi with evading IDS

The authors started their penetration testing with the first method and only when they found that there was IDS installed on the website network, they utilised the second method. According to their testing, 67 e-commerce websites were vulnerable, 21 vulnerable websites were banking websites, 14 were educational institutions, 3 were brokerage houses and 2 were insurance companies.

In one of the largest vulnerability assessments in Bangladesh, Alam et al. analysed 900 websites having the .bd domain for SQLi (Structured Query Language Injection) vulnerability [14]. For their analysis they conducted the assessment using different types of SQLi methods such as:

One single quote (')

One single quote with a bracket ('))

One double quote (")

One double quote with a bracket ("))

One backslash (\)

Among the analysed websites, 600 were found to be vulnerable. Among the vulnerable ones, 510 were vulnerable to ‘get based SQLi’ and the rest 90 were vulnerable to ‘post based SQLi’. Also, about 70% of the vulnerable websites were were vulnerable to single quote, 15% could be exploited using a single quote bracket, 10% were vulnerable against a backslash SQLi method, whereas 5% were exploitable using a double quote method.

Adil et al. evaluated different aspects of password adoption in 36 Bangladeshi Government websites against a set of 6 heuristics [15]. The heuristics are:

H1 Password construction guidelines

H2 Password recovery

H3 Use of CAPTCHA

H4 Security question

H5 HTTPS Channel and

H6 Password strength meter

These six heuristics represent the guidelines that are essential for different aspects of passwords. For each selected websites, the authors investigated if the website satisfied each heuristic. Their work reported many interesting findings as discussed next. Only 13 websites (36%) satisfied the H1 heuristic where H2 was satisfied by all 36 websites (100%). On the other hand, the heuristic completion numbers for H3, H4, H5 and h6 are 16 (44%), 4 (11%), 17 (47%) and 1 (0.03%) respectively. The finding regarding H6 is quite surprising indeed. A password strength meter is crucial for helping users to select a strong and secure password. Only 1 website adopted such a method during their study.

The need for policies to ensure security and privacy in the banking sector of Bangladesh was highlighted in a study presented by Khan et al. [16]. The study collected data from two sources: primary and secondary. For collecting primary data, a questionnaire of 40 questions were sent to 15 banks in Bangladesh and 11 banks returned their responses. The authors used online and physical sources to collect secondary data. Some of the finding of the survey are:

67% of the surveyed banks reported that they had proper adequate knowledge for ensuring state-of-the-art security.

56% of the surveyed banks reported that there was lacking for proper security training.

55% of the surveyed banks reported that they did not have quick response capability in case of an emergency situation.

44% of the surveyed banks thought the Government was not very active in responding to emergency situations.

Afterwards, the authors presented a set of recommendations on how to improve the situations. The study provides unique observations, however, the main limitation is that it was conducted in 2009. There have been a lot of technical advancements in the last decade in Bangladesh in different sectors including the banking sector. Therefore, many of findings might not be relevant anymore.

Sadekin et al. discussed different security measures for e-Banking in Bangladesh [17]. In addition, the authors also conducted a survey from 120 participants. The participants included 44 bank employees and 76 bank customers with 28 from rural areas whereas the rest (92) from urban areas, thus covering a wide range of demographics. Among the respondents, 28.3% did not maintain any e-banking accounts. The survey also consisted of a study of passwords which revealed that 31.7% of respondents only used digits as their passwords, while 18.3% used name or letter and 18.3% used some digits and some letters. There are some other interesting insights from their study:

They found a positive correlation between the location of banking ATMs and security of e-banking.

They reported a positive correlation between hacking of accounts and password sharing.

They reported a positive correlation between hacking of accounts and not using any Anti-virus software.

Many respondents believed that the e-banking in Bangladesh highly secured (15%) or sufficiently secured (41.7%) whereas 31.7% considered not enough secured.

Many respondents (51.7%) reported that they did not regularly log out from online banking accounts.

The limitation of the study is that they just reported their findings and did not provide any recommendation.

A SQLi (Structured Query Language Injection) vulnerability assessment of 359 educational websites was reported by Alam et al. [18]. The assessment was conducted using manual black box testing in which they considered different SQLi methods such as:

Normal SQLi

Error based/double query injection

Blind injection

Among of the 359 websites, 309 websites were found to be vulnerable to at least one of the SQLi methods. Among them, normal SQLi affected 199 websites while 87 websites were affected by error based or double query injection method. The SQLi type for the rest of websites (24) could not be identified. The authors also claimed that they were able to achieve to full database access for 79 vulnerable websites. Also, they were able to retrieve different database tables in 120 websites.

Sarkar et al. conducted a qualitative comparative analysis different cyber security strategies of Bangladesh [19]. The comparison was carried out using the following criteria:

Promoting cyber security R&D

Promoting cyber security education

Ensuring on going risk assessment

Promoting counter cybercrime policy

Promoting cyber security in International law

Forms of regulation and institutional aspects

Balancing cyber security with civil liberties

Types of cooperation

The authors also compared different aspects for each of these criteria with other countries. Finally, they provided some recommendations.

A large study of passwords and other security aspects while using online services in Bangladesh is presented by Khan et al. [1]. The study consisted of a survey which utilised a questionnaire consisting of two demographic and eighteen information related questions. The survey was conducted among 1682 users within a period of three months, September 2014 to December 2014. Some of their findings are presented below:

72.2% users used similar passwords. 7.7% users never changed their passwords and 74.1% seldom changed their passwords.

62.5% users saved their passwords while accessing online services with 57.9% users preferring automated sign-in while accessing online services.

Being aware of the privacy implications, 34.3% users did not allow Facebook apps to access their data from Facebook.

51.6% users were glad to re-enter authentication information while accessing online services while 28.6% users were annoyed with re-authentication mechanisms.

13.3% users reported of their accounts being hacked and 16.4% users mentioned that when they shared data online those data had been misused.

The study also investigated privacy awareness. Surprisingly, 76.9% users did not check the website authenticity before providing any private information. However, 64.8% users used privacy settings and 9.9% never used any privacy setting.

4. REVIEW OF PRIVACY WORKS

There have been a few studies in Bangladesh focusing on data privacy. For example, Hossain et al. presents a study on data privacy from the perspective of Bangladesh [20]. They identified three main stakeholders: consumer, industry and Government; who might impact the current state of data privacy in Bangladesh. Therefore, they aimed to know the view of consumers and to understand the point of view of the industry experts regarding data privacy and to analyse the Governments initiatives to protect data privacy. The key findings along with the limitations of the paper are:

Consumers' Perspective: To understand the consumers perspective, they conducted a survey among 81 respondents, who were mainly university students. They asked each respondent's gender, age range, Internet usage, data privacy knowledge, importance of data privacy, concern on data privacy while purchasing online and visiting any website throughout the survey. The results show that 63.0% of respondents felt that data privacy was very important to them. However, around 54.4% respondents stated that they were not concerned about privacy while doing any online shopping.

Industry Perspective: Private companies did not require to declare their privacy policy publicly. They only needed to provide documents mentioning their existing systems and operations as parts of documentations. One of the managers from an IT company said that they did not need to follow any generalised rule regarding any privacy policy for BPO (Business Process Outsourcing).

Government Perspective: Towards the vision of "Digital Bangladesh", the Government of Bangladesh has expanded cellular subscriptions, digitised state-related activities, such as e-TIN registration, Machine Readable Passport (MRP), access to public information and many more. To ensure the cyber-security, the Government endorsed the Digital Security Act, 2016, however, the Government had not proposed any formal regulation or policy on data privacy.

The limitation of the study is that it is not well defined and well represented. Also, the sample of the survey is very low and only university students were the major participants which created a bias in the study. Further, the recent law enforcement regarding digital privacy are not mentioned or studied. The authors recommended that the definition of personal data should be clearer in the new proposed law as it was not clearly mentioned in the Data Protection Law of Bangladesh. They also proposed that it was important to have a clear purpose for processing personal data and punishment should be enforced for obtaining, transferring or selling of personal data without any lawful authority.

In another research [21], Haque et al. identified privacy vulnerabilities in commercial Digital Service Centers (DSCs) in Dhaka, Bangladesh. The authors presented findings from a 6-month long ethnographic study in 19 DSCs which included two types of shops: Computer Service Shop (CSS) and FlexiLoad Shop (FLS), situated in Dhaka, Bangladesh. The data were obtained from the ethnographers' observations, contextual inquiries, and interviews with 44 shopkeepers and 64 customers. By analysing these data, the authors provided an overview of privacy vulnerabilities in public DSCs in Bangladesh and analyzed the vulnerabilities through the lens of informal markets or bazaars in developing countries.

According to their analysis, infrastructural limitations, local power politics, lack of knowledge, and insufficient protection mechanisms are the main reasons to create privacy vulnerabilities for the customers of these centers. The authors reported that the concepts of clientelisation, reputation, and situated morality on informal markets to demonstrate that privacy vulnerabilities in DSCs were associated with broader contexts of development, culture, informality, and postcolonial computing and privacy. The authors offered a few suggestions to mitigate the privacy vulnerabilities created in DSCs:

> Designers and policy makers could focus on reputation-based accountability, communal surveillance, and empowerment of DSCs to re-design the privacy mechanism in these DScs.
>
> As the DSCs provide paying services to their customers, these should maintain customer privacy and protect personal and sensitive information.
>
> Proper authorities need to be careful to develop and give permission to a robust infrastructure before introducing a new digital service. Otherwise, many citizens may suffer from a technology breakdown.

Another research work, published by Khan et al. [22], presented a brief overview of security and privacy issues of integrated healthcare information system in Bangladesh. The risk of privacy violation is high, as the Government of Bangladesh is implementing the National Health Data Warehouse in the country. Due to easy online access, Bangladeshi citizens are a potential target of cyber criminals. The authors designed and proposed a practical solution, Patient De-Identification with Linkage Preservation (PDLP), that anonymised the identifiable personal data of existing billions of medical records and maintained a record linkage as well. They encrypted the personal information such as mobile numbers, gender and name-values to produce anonymised and linkable patient identification key. The authors claimed that using their solution, patients data could be shared and integrated with different public and private hospitals and diagnostic centres in the country. They also claimed that their system had been implemented to develop National Health Data Warehouse in Bangladesh.

The proposed system is quite straight-forward, however, the major issue of the system is with the patient's mobile number. In Bangladesh, it is quite common to have multiple mobile numbers of the patients. A patient can provide one contact number in a health centre and another contact number in a different health centre which can create two different individuals data in the warehouse database system. Therefore, it may hamper the data mining results.

Two research works by Ahmed et al. and Guha et al. examined the privacy risks associated with the practice of repairing broken digital artifacts in Bangladesh [23, 24]. The authors conducted an ethnographic study to explore privacy vulnerabilities identified during the repair process. They also analysed peoples perceptions toward privacy in repair and its connections with the social and cultural values in a broader way.

From a three-month ethnographic study followed by an online survey, the authors pointed out the following main concerns around privacy in repair:

> Privacy had been threatened at repair workshops in Bangladesh. It was evident in the research that repairers accessed customers' personal data and shared with others without customers consent.
>
> People were skeptical about using any encryption based technical solution and they believed that these kind of solutions would not work in Bangladesh as clients needed to share their passwords with the repairers.
>
> People were unsure and confused to impose laws and/or policies to preserve the privacy of their personal data during the repair process.
>
> Religious and cultural values might positively affect the privacy in repair ecosystem.

The authors urged that the privacy vulnerability was closely associated with information and communication technologies and this issue was not researched properly yet, particularly in technology and developmental contexts.

An interesting study investigating the security and privacy implications while registering for new mobile SIMs using Biotmetric in Bangladesh is presented by Ahmed et al. [25]. During the study, the authors conducted 30 interviews with mobile registration operators and 34 interviews with customers where each interview was 15 minutes long. In addition, the authors alos visited 30 families and conducted semi-structured interviews. In addition to these interviews, they also conducted an online survey which resulted in 606 responses. Some of the findings emerging from their study are presented below:

> There were concerns in the identity verification process as many users did not have any proper ID card. In such cases, people sometimes used the ID cards of their relatives which clearly defeats the whole purpose of identity verification during SIM registration.
>
> Many people expressed their concerns of exploitation of their biometric data either by the Government or some malicious actors.
>
> The authors also reported their concerns regarding the biometric process itself as any registration operator can act maliciously to capture sensitive biometric data.
>
> From the survey response, 77% respondents expressed that they did not like the biometric registration process while 15% users were supportive.

Ahmed et al. [26] presented another research where digital privacy challenges with shared mobile phone use in Bangladesh were studied. The authors conducted a qualitative study to analyse how families in Bangladesh shared their mobile phones and to evaluate the privacy challenges that might arise when the individuals needed to protect their personal data privacy.

Sharing mobile devices with different family members is a common social practice in Bangladesh due to economic need, running out of battery or airtime balance. A set of three sharing models were considered: sharing between a husband and wife, sharing between siblings and sharing between parents and children. The authors took semi-structured interviews with 72 participants from 38 families in Dhaka, Bangladesh. The study revealed that mobile device sharing users were not always happy in sharing and they wanted to keep their information private and wanted a personal space, however, it was not always possible to find such a personal space. This created a complexity of revealing and hiding private information. The study also revealed that power relationships affected sharing practices and impacted the privacy of wives' data. The same authors proposed a solution to create an experimental system that would enable a single user with multiple accounts in [27]. This prototype, called *Nirapod*, would allow a person to create a 'shared' account and a separate 'secret' account. Using the 'shared' account, the other family members would access the data using a password or a PIN code. On the other hand, the 'secret' account would contain all the personal data that the main user would not share with the others. The authors conducted a three-week field study of the implemented prototype with 21 participants in Dhaka, Bangladesh. The study revealed that the women participants were more concerned about their personal privacy and they were interested in new apps like *Nirapod* that could provide better privacy.

5. DISCUSSION

We have analysed 19 research works which mainly focus on the Bangladesh specific security and privacy issues covering a wide-range of application domains and study areas. Our analysis of these review works have been summarised in Table 1 and Table 2. Table 1 provides application centric summary of analysed works using application taxonomy (Figure 1) whereas Table 2 presents a study-centric summary of the reviewed works according to the study taxonomy (Figure 2). In these table, "●" notation has been used to denote if a particular works deals with the criterion of the corresponding column whereas the symbol "○" has been used to denote that the criterion of the corresponding column is *not applicable* for the respective work. Both these tables provide a visual comparative analysis of the reviewed works, allowing any reader to easily understand the scopes of our review. Different areas of researches in security and privacy along with the number of papers are presented in Figure 3.

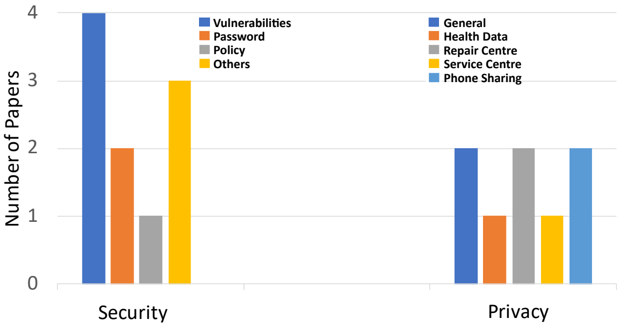

Fig. 3. Security and Privacy Study Summary

6. CONCLUSION

In this study, we have thoroughly analysed 19 research works focusing different security and privacy issues and solely conducted in the context of Bangladesh. To conduct our reviews, we have adopted two taxonomies, application and study taxonomy, each of which has been categorised further. Afterwards, we have reviewed the selected works. Finally, we have utilised the taxonomies to present a comparative analysis of the reviewed works in tabular formats so as to provide an easy to understand visual analogy of the reviewed works. The main motivation is that such a survey will act as the foundation for anyone who would like engage in Bangladesh specific security and privacy researches in years to come.

7. REFERENCES

[1] Rasib Khan and Ragib Hasan. Security-aware passwords and services usage in developing countries: A case study of bangladesh. In *International Conference on Services Computing*, pages 67–84. Springer, 2018.

[2] Bangladesh Telecommunication Regulatory Commission. Internet Subscribers Bangladesh, October 2020, (accessed December 1, 2020). `http://btrc.gov.bd/content/internet-subscribers-bangladesh-october-2020`.

[3] Sam Thielman. Yahoo hack: 1bn accounts compromised by biggest data breach in history. *The Guardian*, 15:2016, 2016.

[4] Kimberly A Whitler and Paul W Farris. The impact of cyber attacks on brand image: Why proactive marketing expertise is needed for managing data breaches. *Journal of Advertising Research*, 57(1):3–9, 2017.

[5] Ashish Garg, Jeffrey Curtis, and Hilary Halper. Quantifying the financial impact of it security breaches. *Information Management & Computer Security*, 2003.

[6] Atreyi Kankanhalli, Hock-Hai Teo, Bernard CY Tan, and Kwok-Kee Wei. An integrative study of information systems security effectiveness. *International journal of information management*, 23(2):139–154, 2003.

[7] David Wright, Rachel Finn, and Rowena Rodrigues. A comparative analysis of privacy impact assessment in six countries. *Journal of Contemporary European Research*, 9(1), 2013.

[8] Ralph Gross and Alessandro Acquisti. Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pages 71–80, 2005.

[9] Aditya Vashistha, Richard Anderson, and Shrirang Mare. Examining security and privacy research in developing regions. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies*, pages 1–14, 2018.

[10] Tanjila Farah, Moniruzzaman Shojol, Maruf Hassan, and Delwar Alam. Assessment of vulnerabilities of web applications of bangladesh: A case study of xss & csrf. In *2016 sixth international conference on digital information and communication technology and its applications (DICTAP)*, pages 74–78. IEEE, 2016.

[11] Md Moniruzzaman, Farida Chowdhury, and Md Sadek Ferdous. Measuring vulnerabilities of bangladeshi websites. In *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, pages 1–7. IEEE, 2019.

[12] Afsana Begum, Md Maruf Hassan, Touhid Bhuiyan, and Md Hasan Sharif. Rfi and sqli based local file inclusion vulnerabilities in web applications of bangladesh. In *2016 International Workshop on Computational Intelligence (IWCI)*, pages 21–25. IEEE, 2016.

[13] Tanjila Farah, Delwar Alam, Md Alamgir Kabir, and Touhid Bhuiyan. Sqli penetration testing of financial web applications: Investigation of bangladesh region. In *2015 World Congress on Internet Security (WorldCIS)*, pages 146–151. IEEE, 2015.

[14] Delwar Alam, Md Alamgir Kabir, Touhid Bhuiyan, and Tanjila Farah. A case study of sql injection vulnerabilities assessment of. bd domain web applications. In *2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec)*, pages 73–77. IEEE, 2015.

[15] Adil Ahmed Chowdhury, Farida Chowdhury, and Md Sadek Ferdous. A study of password security factors among bangladeshi government websites. IEEE, 2020.

[16] Muhammad Saifuddin Khan and Suborna Barua. The status and threats of information security in the banking sector of bangladesh: Policies required. *Bangladesh Journal of MIS*, 1(2), 2009.

[17] Mohammad Shamsus Sadekin and Md Abdul Hannan Shaikh. Security of e-banking in bangladesh. *Journal of Finance and Accounting*, 2016.

[18] Delwar Alam, Touhid Bhuiyan, Md Alamgir Kabir, and Tanjila Farah. Sqli vulnerabilty in education sector websites of bangladesh. In *2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)*, pages 152–157. IEEE, 2015.

[19] Kaushik Sarker, Hasibur Rahman, Khandaker Farzana Rahman, Md Arman, Saikat Biswas, Touhid Bhuiyan, et al. A comparative analysis of the cyber security strategy of bangladesh. *arXiv preprint arXiv:1905.00299*, 2019.

[20] Kamal Hossain, Khabirul Alam, and Umme Saara Khan. Data Privacy in Bangladesh: A Review of Three Key Stakeholders Perspectives. In *Seventh International Conference on Advances in Social Science, Economics and Management Study - SEM 2018*, pages 46–50. IRED, 2018.

[21] SM Taiabul Haque, MD Romael Haque, Swapnil Nandy, Priyank Chandra, Mahdi Nasrullah Al-Ameen, Shion Guha, and Syed Ishtiaque Ahmed. Privacy vulnerabilities in public digital service centers in dhaka, bangladesh. In *Proceedings of the 2020 International Conference on Information and Communication Technologies and Development*, pages 1–12, 2020.

[22] Shahidul Islam Khan and Abu Sayed Md Latiful Hoque. Development of national health data warehouse bangladesh: Privacy issues and a practical solution. In *2015 18th International Conference on Computer and Information Technology (ICCIT)*, pages 373–378. IEEE, 2015.

[23] Syed Ishtiaque Ahmed, Shion Guha, Md Rashidujjaman Rifat, Faysal Hossain Shezan, and Nicola Dell. Privacy in repair: An analysis of the privacy challenges surrounding broken digital artifacts in bangladesh. In *Proceedings of the Eighth International Conference on Information and Communication Technologies and Development*, pages 1–10, 2016.

[24] Shion Guha, Mohammad Rashidujjaman Rifat, Faysal Hossain Shezan, Nicola Dell, et al. Privacy vulnerabilities in the practices of repairing broken digital artifacts in bangladesh. *Information Technologies and International Development*, 2017.

[25] Syed Ishtiaque Ahmed, Md Romael Haque, Shion Guha, Md Rashidujjaman Rifat, and Nicola Dell. Privacy, security, and surveillance in the global south: A study of biometric mobile sim registration in bangladesh. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 906–918, 2017.

[26] Syed Ishtiaque Ahmed, Md Romael Haque, Jay Chen, and Nicola Dell. Digital privacy challenges with shared mobile phone use in bangladesh. *Proceedings of the ACM on Human-Computer Interaction*, 1(CSCW):1–20, 2017.

[27] Syed Ishtiaque Ahmed, Md Romael Haque, Irtaza Haider, Jay Chen, and Nicola Dell. " everyone has some personal stuff" designing to support digital privacy with shared mobile phone use in bangladesh. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2019.

Table 1. Application-oriented Comparative Analysis.

Research Works	Web Application	Mobile Application	Social Application	Others
Farah et al.[10]	General	○	○	○
Moniruzzaman et al. [11]	General	○	○	○
Begum et al. [12]	General	○	○	○
Farah et al. [13]	Financial	○	○	○
Alam et al. [14]	e-Commerce, Financial, Educational	○	○	○
Adil et al. [15]	Government	○	○	○
Khan et al. [16]	Financial	○	○	○
Sadekin et al. [17]	Financial	○	○	○
Alam et al. [18]	Educational	○	○	○
Sarker et al. [19]	○	○	○	Strategy
Khan et al. [1]	General	○	○	○
Kamala et al. [20]	○	○	○	General data privacy
Haque et al. [21]	○	○	Service centre privacy	○
Khan et al. [22]	○	○	○	Healthcare
Ahmed et al. [23]	○	○	Repair privacy	○
Guha et al. [24]	○	○	Repair privacy	○
Ahmed et al. [25]	○	SIM Registration	○	○
Ahmed et al. [26]	○	Mobile sharing	○	○
Ahmed et al. [27]	○	Mobile sharing	○	○

Table 2. Study-oriented Comparative Analysis.

Research Works	Security				Privacy				
	Vulnerability	Password	Policy	Others	General	Health Data	Repair	Service/Flexiload	Phone Sharing
Farah et al.[10]	XSS, CSRF	○	○	○	○	○	○	○	○
Moniruzzaman et al. [11]	XSS, CSRF, BAS, TLS, Ports, SQLi	○	○	○	○	○	○	○	○
Begum et al. [12]	LFI	○	○	○	○	○	○	○	○
Farah et al. [13]	SQLi								
Alam et al. [14]	SQLi	○	○	○	○	○	○	○	○
Adil et al. [15]	○	●	○	○	○	○	○	○	○
Khan et al. [16]	○	○	●	○	○	○	○	○	○
Sadekin et al. [17]	○	○	○	●	○	○	○	○	○
Alam et al. [18]	SQLi	○	○	○	○	○	○	○	○
Sarker et al. [19]	○	○	○	●	○	○	○	○	○
Khan et al. [1]	○	●	○	●	○	○	○	○	○
Kamala et al. [20]	○	○	○	○	●	○	○	○	○
Haque et al. [21]	○	○	○	○	○	○	○	●	○
Khan et al. [22]	○	○	○	○	○	●	○	○	○
Ahmed et al. [23]	○	○	○	○	○	○	●	○	○
Guha et al. [24]	○	○	○	○	○	○	●	○	○
Ahmed et al. [25]	○	○	○	○	●	○	○	○	○
Ahmed et al. [26]	○	○	○	○	○	○	○	○	●
Ahmed et al. [27]	○	○	○	○	○	○	○	○	●