A FRAMEWORK FOR SECURING PERSONAL DATA SHARED BY USERS ON THE DIGITAL PLATFORMS

Nirjhor Anjum [1], Lamia Islam [2], Md Rubel Chowdhury [3], Ariful Alam [4]

[1] Researcher, SCIT, University of the Cumberlands, Williamsburg, KY, USA
[2] Doctoral Researcher, PPPA, Washington State University, Pullman, WA, USA
[3] Researcher, SCDM, London Metropolitan University, London, UK
[4] Doctoral Researcher, CGPS, Trine University, Hamtramck, MI

ABSTRACT

Public disclosure of private data such as mobile phone numbers, dates of birth, identity card information, and financial data on social websites represents a significant threat to cybersecurity. Both external and internal intrusions infringe on users' privacy, and the available security practices are not preventing unauthorized access. Substandard encryption, poor access controls, and weak policy enforcement form the core deficiencies of handling private data in this study. An in-depth analysis, comprising industry surveys, interviews with experts, and case studies of eCommerce and digital service companies, is carried out to assess the prevailing practices and their shortcomings. It is seen that most of the companies do not have adequate policies and technical measures, and user data is extremely susceptible to misuse. To fill this gap, a Citizen Digital Identity Portal (CDIP) is envisioned as an eGovernance project sponsored by the government. This solution combines encryption, access controls, and API-based identity confirmation to enable companies to confirm user identities without revealing or holding personal information. The threat of abuse by both internal and external entities is therefore greatly minimized. The study concludes that companies cannot guarantee data security alone and that a policy-driven centralized model must be in place. The CDIP model helps bridge the gap between technology and cybersecurity rules. It offers a flexible and powerful way to protect personal information in today's digital world.

KEYWORDS

Personal Data Security, Cybersecurity Framework, e-Governance and Data Protection, Data Privacy Regulations, Secure Digital Identity

1. INTRODUCTION

Personal data security poses a significant challenge in today's technological landscape, with hundreds of incidents occurring globally each day involving the leakage, disclosure, alteration, destruction, tampering, and misuse of personal information. The main reason for these problems is that there are no clear rules for how this data is collected, stored, and used. Both public and private entities, whether registered or not, embark on projects that involve extensive sharing of personal data, often neglecting the security of customer information.

This paper aims to establish a technological framework that safeguards personal data from widespread misuse by public-private ventures and projects. The framework will be developed within the realms of e-Governance and Cybersecurity, with a specific focus on Data Security.

In the initial part of this paper, the research objectives, background, and methodology will be discussed. The next part of this paper will involve an empirical study shedding light on how data is leaked, distorted, and misused. This study will also explore efforts made by certain companies

DOI: 10.5121/ijcnc.2025.17301

to secure data and the challenges encountered. Through the identification of challenges and issues, solutions will be derived as anticipated. The study will utilize methods such as questionnaires, interviews, and case analyses. At least five e-Commerce and Digital Service companies will be surveyed, and at least five senior-level technology officers from these companies will be interviewed.

Following a thorough analysis of real-world scenarios and challenges in data security within the industry, the next part of the paper will be dedicated to designing and explaining the proposed framework. Finally, in the last part of this paper, potential future work in this area will be outlined to pave the way for further advancements in research.

2. OBJECTIVE OF THE RESEARCH

Given the considerable risk and potential financial harm associated with the leakage of personal data, this research paper aims to establish an effective framework for securing personal data on web platforms.

This research paper looks at how businesses today collect, use, handle, and share personal data. It explores the risks inherent in existing practices and examines measures implemented by select companies to enhance data safety. Ultimately, the paper identifies how e-Governance initiatives can regulate public and private endeavors and establish a framework ensuring the safe protection of user personal data, allowing its use by relevant entities.

The primary objective is not to shield public or private initiatives from utilizing users' personal data, a necessity for providing services to customers. Instead, the aim is to manage this process within an ecosystem where public-private ventures and their personnel cannot openly access such data. Even in the event of system breaches, the data should remain secure.

The success of the framework requires government involvement, necessitating the initiation of an e-Governance project focused on cyberspace data safety.

The anticipated outcome of this framework is the creation of a secure ecosystem where individuals can share their personal information safely on any web platform. Web platforms can utilize this information for their business or organizational purposes but will be restricted from open access by staff or intentional/unintentional misuse of the data.

3. BACKGROUND STUDY AND CONTEXT

Protection of individuals' details has been a priority right from the beginning of internet usage. Ever since web technology came into being, experts have worked to keep individuals' confidential information away from hackers and cyber criminals. These criminals try to get details from websites and use them for their nefarious actions. Most people set weak passwords based on easily identifiable facts about themselves like their birth date, nickname, or gender. This makes it convenient for hackers to get into their accounts. Others also use identical passwords for various accounts, such as their email and banking accounts, which makes it even more likely that their accounts can be hacked.

Another issue that is serious is when companies pass on customer information to partner businesses. In other cases, the users consent to it when signing up but don't bother to read the lengthy "terms and conditions." Despite the first company guarding the information, the other businesses may not have such strict regulations, so the data gets abused.

There have been many times when personal data has been stolen. In 2013, The Guardian reported that the National Security Agency (NSA) was gathering smartphone records from millions of Verizon customers [7]. RadioShack bankrupted in 2015, and data from over 100 million customers was sold, leading to legal complications [2]. In 2015, hackers attacked the US Office of Personnel Management and exposed the personal information of 22.1 million people [10]. Another high-profile instance was the Ashley Madison hack, in which hackers revealed 37 million users' personal information in 2015 [8][6]. In 2016, Yahoo reported that hackers had stolen data from 500 million accounts two years previously [9].

These cases indicate how catastrophic personal data leaks are, and there needs to be more research on this topic. Even though most countries have laws to protect personal data, these types of data breaches still happen quite often [11][4]. Such security breaches harm millions of individuals annually. This makes it extremely necessary to develop improved methods of securing data and avoiding cyber-attacks.

In 2024, cyberattacks continued to be a top issue, targeting millions of individuals and businesses across the globe. One of the most devastating attacks was that on Change Healthcare in February 2024. BlackCat (ALPHV) ransomware gang breached the system of this US healthcare payment firm. Due to this, hospitals and pharmacies were unable to process medical bills. A few patients were forced to pay their medical bills out-of-pocket. The attack led to $2.87 billion in losses for the company, and they had to give $6 billion in financial support to the hospitals and the doctors. This attack demonstrates that cyberattacks in healthcare can endanger patients and hospitals must have enhanced cybersecurity. [1] [12]

Another huge attack occurred in May 2024, when Snowflake, a cloud data platform, was breached. Scattered Spider, a cybercrime organization, breached customer data at AT&T, Ticketmaster, and Santander Bank. The hackers gained access by stealing an employee's login credentials. The hackers then demanded ransoms of between $300,000 and $5 million from breached companies. The breach showed that there must be more robust password protection and multi-factor authentication (MFA) to prevent hackers from getting into online networks [1].

The UK Ministry of Defence (MoD) had also been hacked in May 2024. A payroll system that had personal information of 270,000 armed forces members was the target. The stolen information included names, bank account numbers, and home addresses. Most specialists believe that the foreign state could have been behind the attack, though this was not established by the UK government. This incident indicated that even governmental institutions could be vulnerable and in need of more sophisticated security measures. [1] [13]

All these examples indicate that cyberattacks are becoming more perilous. Cyber attackers now aim for vital sectors such as the healthcare industry, cloud computing, and government networks. Despite numerous laws and security policies, hackers continue to infiltrate and steal data. Governments and companies need to implement more robust security measures, guard passwords more carefully, and educate individuals on recognizing cyberattacks to prevent such attacks.

Recent research also emphasizes the importance of lightweight and scalable intrusion detection approaches using clustering algorithms to effectively monitor high-traffic networks, reinforcing the relevance of our proposed framework for large-scale digital ecosystems [14].

It was speculated by many that a foreign nation might have been responsible for the attack, but the government did not confirm this. This attack showed that even governmental agencies are vulnerable and need to have more robust security systems [1]. These incidents show that cyber

threats are getting riskier. Hackers now attack vital sectors such as healthcare, cloud services, and government networks.

Despite numerous laws and security protocols already in place, hackers continue to steal information. To prevent these attacks, organizations and governments need to implement stronger security measures, more securely guard passwords, and educate individuals to recognize cyber threats.

4. RESEARCH METHODOLOGY

This study employs a comprehensive research approach, incorporating a Survey Method, detailed Interview Method, and Case Study analysis. The objective is to scrutinize industry practices concerning the collection, utilization, potential misuse, attempted safeguards, and the challenges faced in safeguarding personal data.

Initially, a meticulously crafted set of questions was administered to 5 ecommerce companies. To extract insightful responses, senior officials from these companies, possessing valuable insights, were selected. The questionnaire, tailored to elicit nuanced information, served as an initial step in understanding data safety measures and the challenges encountered by industry professionals. While the Survey Method provided a foundational understanding, it proved insufficient in uncovering all intricacies and potential solutions. [3]

To delve deeper into the challenges of Personal Data Safety, a detailed Interview Method was employed. Engaging senior officials in interviews provided a clearer comprehension of the nuances surrounding Personal Data Safety. These interviews not only shed light on existing challenges but also offered insights into the strategies adopted by the industry to address Personal Data Safety concerns. However, these insights alone were insufficient for mitigating the challenges posed by Personal Data Safety on web projects. [5]

Subsequently, five Case Studies will be selected from various ecommerce and digital services companies, focusing on aspects such as data protection measures, challenges faced in data security, and instances of data breaches. These case studies are designed to give a detailed understanding of real-life situations related to Personal Data Safety. [5]

All surveys, interviews, and case studies were conducted with senior officials to ensure a comprehensive exploration of real-time Personal Data Safety challenges and potential remedies. This holistic approach aimed to identify the sources, types, scopes, and reasons behind Personal Data Protection Challenges in the industry, leading to the formulation of viable remedies. Ultimately, the culmination of these research methodologies facilitated the development of a technological framework for managing Personal Data Safety on web platforms. [5]

Importantly, the research extended its purview beyond local ecommerce companies to encompass foreign counterparts. This broadened scope ensures a global context, enriching the research findings with diverse perspectives and experiences.

5. FINDINGS OF THE STUDY

5.1. Survey Method Findings

5.1.1. Source of the Data

The data is gathered from senior level experts in the industry, making sure that their feedback is both reliable and fair (Chart 1).

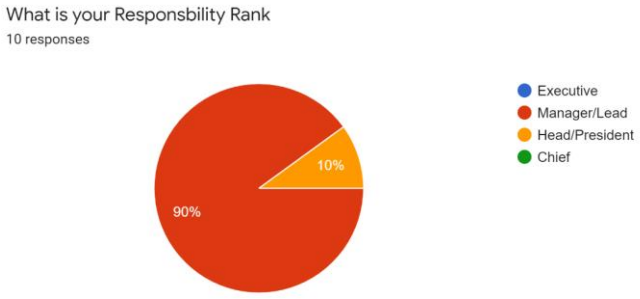

Figure Name: Chart 1

The study involved individuals in leadership roles, specifically team leaders with extensive experience leading development teams ranging from 4 to 21 members (Chart 2). This substantial leadership background underscores the participants' competence to address the subject of Personal Data Safety on Software and Web Platforms.

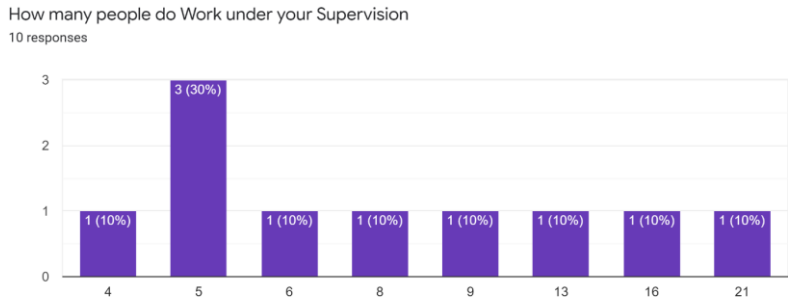

Figure Name: Chart 2

5.1.2. Understanding the Types of Personal Data

Personal data encompasses information utilized for the identification of an individual or the understanding of their interests and behavior. While the loss of personal data may initially appear inconsequential, it has the potential to be exploited by malicious entities, leading to significant disasters in various forms.

According to industry experts, personal data may encompass a range of details such as name, date of birth, gender, father's name, mother's name, mobile number, home address, office address, email address, spending interests, buying behavior, national ID number, driving license number, bank card number, bank account number, profile picture, fingerprint, and other biometric data. If any of these personal details are exposed, it can surely lead to serious problems for the victim, affecting them in both financial and non-financial ways (Chart 3).

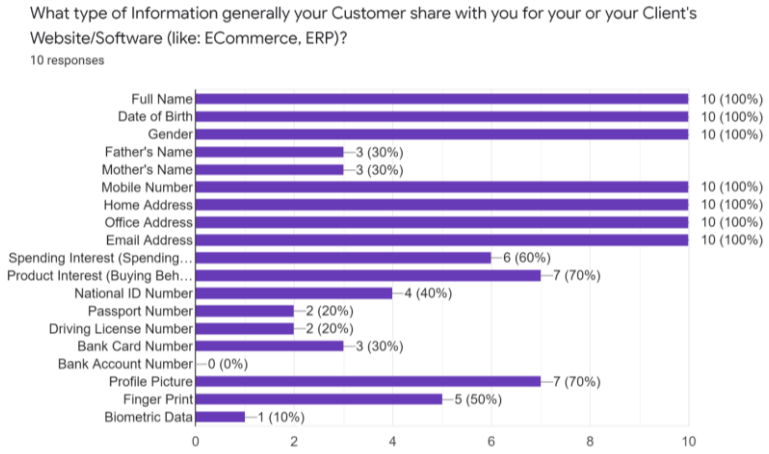

Figure Name: Chart 3

5.1.3. Importance of Personal Data Safety

Every industry expert has emphasized the paramount importance of Personal Data Safety for both users and companies. Specifically, 50% of these experts underscored that it holds equal significance for both users and the companies responsible for delivering software or web platforms to these users (Chart 4).

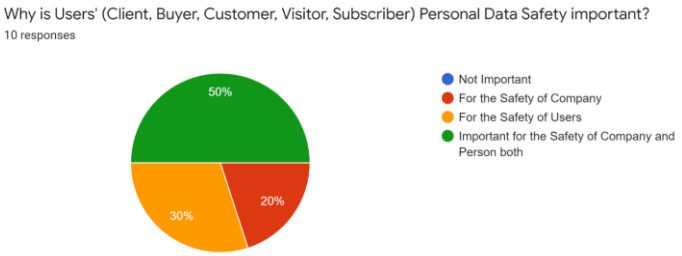

Figure Name: Chart 4

5.1.4. Loss of Users Due to Leakage of Personal Data

All industry experts emphasize that the compromise of users' personal information to unwanted parties poses a significant threat to privacy. Such leaked information can be exploited by malicious entities to impersonate users, potentially leading to the hacking of the victims' digital profiles and assets.

Several experts highlight that the leakage of personal information often results in financial disasters. Hackers can employ tools to compile a list of assumed credentials from the leaked data, attempting unauthorized access to the victims' online financial accounts. This vulnerability is compounded when users use the same credentials across various websites and financial service platforms, making them easy targets for exploitation.

Additionally, some experts assert that data breaches can have repercussions on users' reputations. Unwanted parties may utilize the leaked information to fabricate fake digital profiles, subjecting users to embarrassment or threats. Instances have been observed where blackmailers, armed with gathered personal information, create false profiles, disseminate misinformation online, and subsequently attempt to extort money from victims by leveraging threats. (Chart 5)

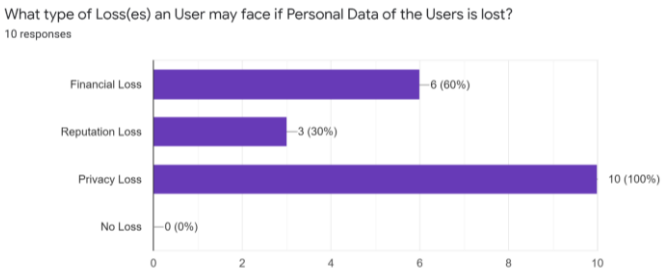

Figure Name: Chart 5

5.1.5. Ways y bwhich Personal Data Might Get Lost

Almost all industry experts have pointed out that the primary cause of personal data leakage is the development of insecure websites and APIs by inadequately skilled individuals. The vulnerability arises when web platforms lack proper security measures, creating a significant risk of personal data being leaked by hackers.

A substantial number of industry experts have observed that most companies neglect the implementation of Data Access and Data Protection Policies for their software and web platforms. This highlights the urgent need for the industry to work together and make user data protection a top priority.

Several experts have highlighted the absence of encryption mechanisms for securing personal information in databases. Consequently, they emphasize that database administrators and application developers have unrestricted access to user data without encryption. In the absence of policy-level or technical constraints to prevent unethical practices, system developers and managers could potentially access and leak personal data. (Chart 6)

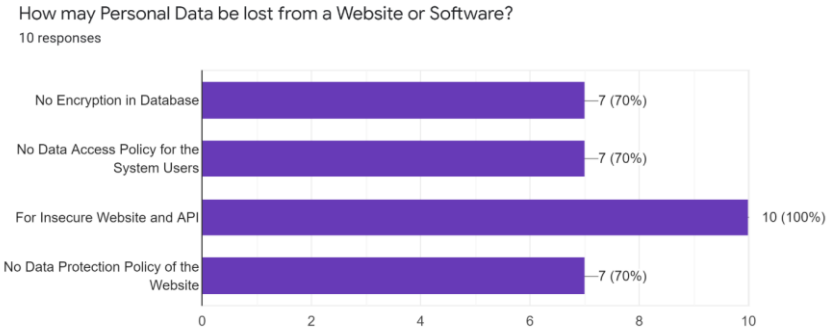

Figure Name: Chart 6

5.1.6. Industry's Technology-Level Practice Regarding Personal Data Safety for the Users of Software and Web Platforms

The responses from industry experts in the questionnaires reveal that most companies rely on technical measures to ensure the safety of their websites, software, and APIs. However, only a small number of companies follow international standard policies for data safety at the technical level, and many companies do not take any policy-level actions to protect users' personal data. (Chart 7)

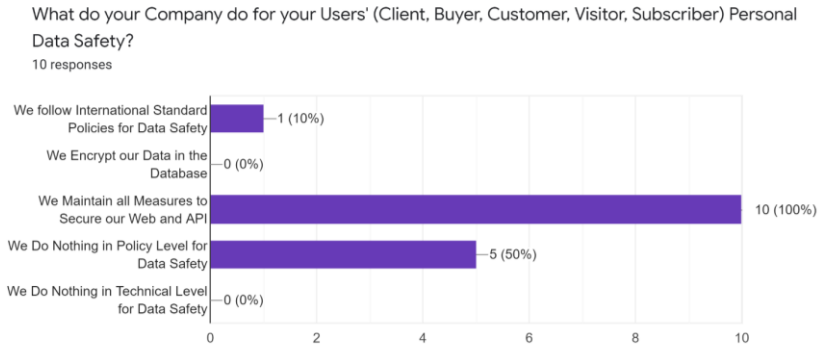

Figure Name: Chart 7

Hence, it is evident that while many companies claim to adhere to technology-level practices for ensuring Personal Data Safety, a majority of them lack awareness regarding international standard policies that could enhance the precision of implementing technological measures for Personal Data safety.

5.1.7. Understanding Technology Platforms and their Features to Ensure Personal Data Safety

The input from industry experts indicates that Content Management Systems (such as WordPress, OpenCart, Magento, Drupal, PrestaShop, NopCommerce) lack technological features to guarantee Personal Data Safety at the system level. (Chart 8)

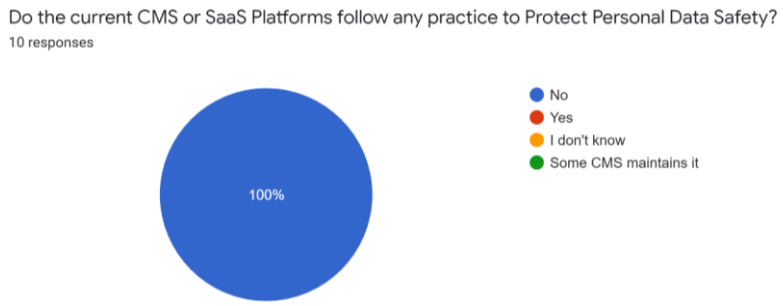

Figure Name: Chart 8

This can be recognized as an inherent limitation wherein the majority of web platforms do not possess the technological capability to safeguard personal data.

5.1.8. Industry's Policy-level Practice regarding Personal Data Safety for the Users of Software and Web Platforms

The participants' direct responses to a specific question unmistakably reveal that the majority of companies do not adhere to international standard policies for ensuring the safety of personal data. (Chart 9)

This underscores a notable gap in the industry's commitment to universally recognized benchmarks for personal data protection. The implications of such non-compliance could extend to heightened risks for both users and the companies themselves.

Figure Name: Chart 9

5.1.9. Understanding Companies and their practices about adopting Standards and Policies to ensure Personal Data Safety

The results from the questionnaire show that many companies fail to provide training to their employees on the important issue of Personal Data Safety. This highlights a noteworthy deficiency in recognizing the importance of educating personnel on safeguarding personal data.

Figure Name: Chart 10

In addition, answers to another question show that about half of the companies do not have a dedicated security auditor or security expert to handle personal data safety on digital platforms. (Chart 11)

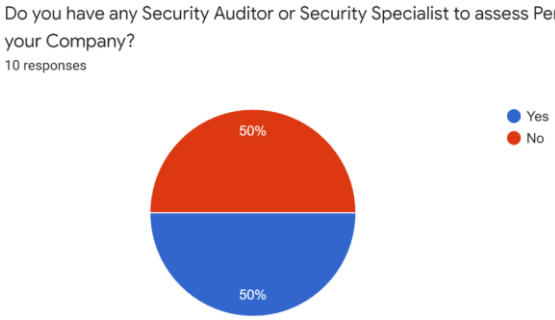

Figure Name: Chart 11

Hence, it is evident that many companies exhibit a limited commitment to implementing policy-level actions that could guarantee Personal Data Safety. This observation underscores a potential

gap in the proactive measures these organizations take to enhance and secure personal data protection.

5.1.10. Suggestion from Industry Expert on Personal Data Safety

Numerous industry experts recommend adhering to international standards by restricting engineers from accessing live project databases. They emphasize implementing features on software and web platforms that limit Site or System Admins' access to only essential personal information for verification or service delivery purposes. (Chart 12)

Figure Name: Chart 12

Experts also suggest that such a limited access policy for personal data safety should not be at the policy level, but the implementation of this policy should occur technically so that, even if any person carries the intention to steal personal data, they would be prevented by the technology. (Chart 13)

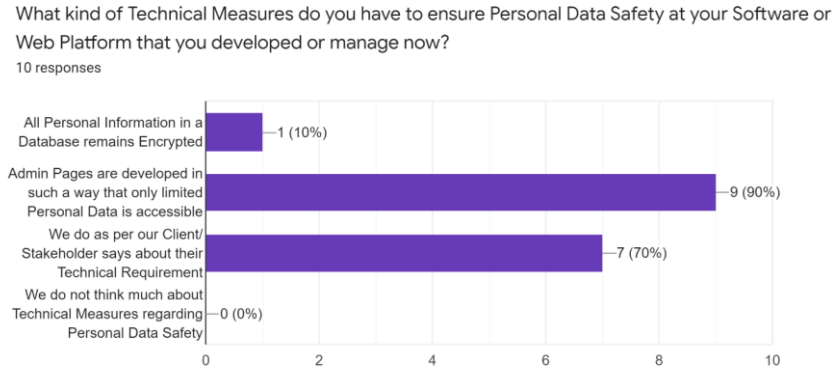

Figure Name: Chart 13

Some industry experts suggested that personal information should be kept in encrypted (unreadable but recoverable) format in the database so that even the database administrators or system administrators may not be able to view personal data who are implementing the personal data protection technologies and policies at the system level. However, since people are using technology to follow policies and protect personal data, it is clear that personal data can never be 100% safe just by using technology and applying policies at the organization or individual level.

Industry experts also suggest that companies should arrange training and create awareness of personal data safety for employees. Besides, all the companies should work at the technology and policy levels to ensure data safety. (Chart 14)

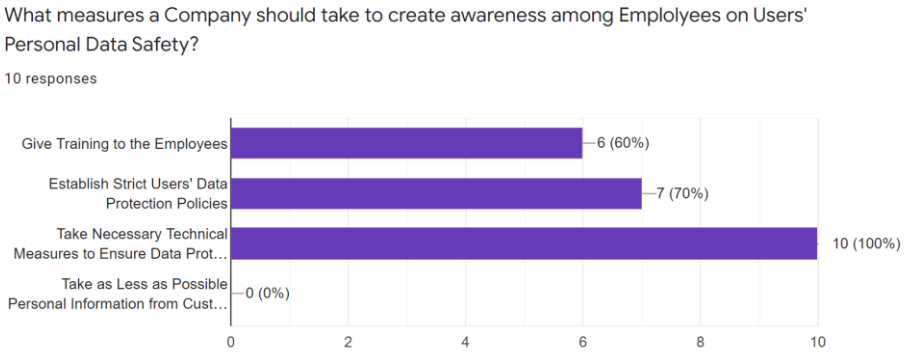

Figure Name: Chart 14

This makes an understanding that, if even policies exist, they cannot protect users' personal data from unwanted people because the adoption of practice depends on the companies, users, their view, and their mindset. There is no guarantee that policy can prevent human action. Therefore, there must be a framework that would combine policies with technologies that drive companies and users in a standard way so that personal data remains safe.

5.1.11. Collecting Feedback from Industry Experts on the success of Personal Data Protection from Company or Individual Level Initiatives

A majority of industry experts stated that it is impossible to protect personal data on all public and private digital platforms if the initiative is taken from the level of that specific company or individual facilitating the software, web, or other digital platform. (Chart 15)

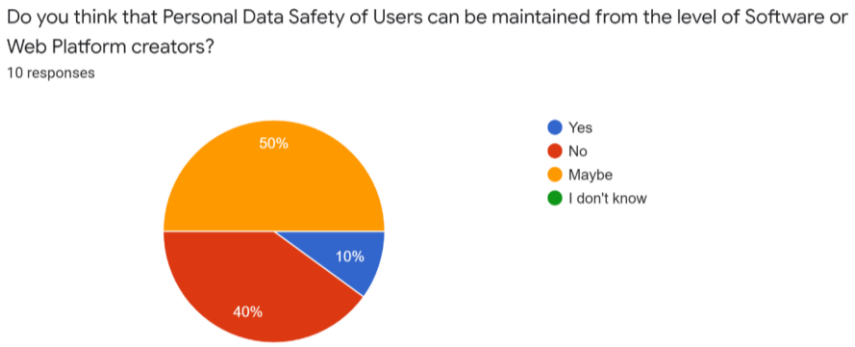

Figure Name: Chart 15

5.1.12. Collecting Feedback from Industry Experts on the Role of eGovernance in Ensuring Personal Data Safety

The consensus among a majority of industry experts is that implementing an eGovernment framework, integrating technology and policies, can effectively guarantee Personal Data Safety across all digital platforms. This unified approach is seen as a comprehensive solution to address

the complexities of data security and privacy, aligning with the evolving landscape of digital interactions and safeguarding personal information. (Chart 16)

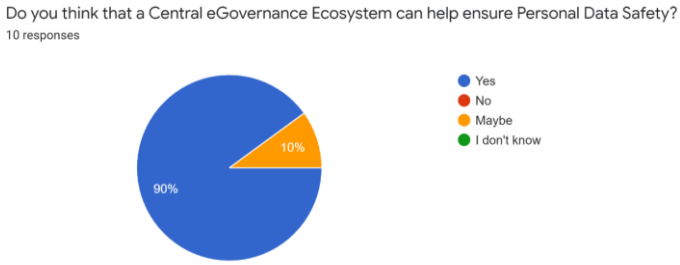

Figure Name: Chart 16

5.2. Interview Method Findings

For the purpose of this research, all of the industry experts were interviewed. However, only a few interviews were presented here, which were found to be truly practical and relevant and were not repetitive feedback.

5.2.1. Interview 1 Findings

While having an interview with the first industry expert, his view was as follows:

> *"I have worked in both foreign and local companies for a long time. Most of them were web-based application development companies making web platforms for their own or their clients. I found that none of the companies train their employees about how to ensure Personal Data Safety. Moreover, many companies were so large, but they still had no cybersecurity specialists who could guide and mentor the teams on personal data safety. However, in the case of developing web projects for our clients or us, we developed the admin panels so that administrative people, the billing department, the sales department, etc., could access clients' personal information openly. There was no restriction in the admin panel, and the personal data were handled openly. They used to check them over the panel and on-demand; they would also download them in the form of Excel. It is possible that someone among them could use this personal data for their own gain or might sell the data to the wrong people just to make some money. In some companies, in a few cases, the stakeholders suggested that they would restrict some of their system users from viewing all of their personal information; however, that was for protecting the safety of their own business, but it is not found that any stakeholder ever shared their requirement to protect personal data of the users. In most cases, a set of personal data protection terms and conditions were just written as a formality for developing the TOC or Privacy Policy page, but nobody used to practice them practically in real life."*
>
> *Interview Dated: July 18, 2024*

5.2.2. Interview 2 Findings

In a second interview, an industry expert stated his experiences and suggestions as follows:

> *"I have been working for a long time in the software industry. I worked in around 5 companies so far. I worked on developing large-scale websites and web portals, mainly where the majority of them were E-Commerce focused. I found that, in the case of most companies, they do not practice Data Privacy Policies at all. Though many things are written*

in their Terms and Policies, these are not managed, monitored, or controlled. The harsh reality is that despite giving training or declaring policies, accidents may occur that may leak the personal information of users from the web platforms because the policies are not controlled with the help of technology. For example, if we tell our staff not to misuse users' personal information, and in case of violating this rule, the specific staff would be punished, there remains a chance that anybody can steal and misuse the personal information. In these situations, only technology can protect personal information. If we put restrictions on the panels, no system user will be able to view a client's personal information, and limited data will be available to verify a user. For example, to verify a user, the call center agents can ask for an order ID and a customer ID rather than asking for the client's mobile number. All the web platforms allow its system users to bulk download mobile numbers and email addresses in the form of Excel files. Next, the system users, generally marketers, use these mobile numbers and email addresses on SMS Gateway and Email Gateways to do SMS and Email marketing campaigns. In such cases, the system user (in this case, the marketer) can use these mobile numbers and email addresses for personal purposes, misuse them, or sell them for little benefit. Alternatively, if the system were integrated with SMS and Email Gateway, the marketer would not be required to download this personal information from the system to do marketing manually. But, as the companies, merchants, and stakeholders do not bother much about personal data safety, they allow downloading and using mobile numbers and email addresses openly, while they know that a marketer may leak these data anytime, which nobody can trace until and unless any technological monitoring is established. I personally have seen companies establish punishing laws in case of leaking personal data while their marketers openly use and share user data. I can say that such incidents will be preventable if personal data safety is centrally controlled with the help of technology, maybe from the government level, because surely it is not possible to control thousands of web platforms just by declaring laws and policies."

Interview Dated: August 25, 2024

5.2.3. Interview 3 Findings

In a third interview another industry expert has stated his experiences follows:

"I have spent many years working in the IT field. I am a CMS developer, and I have found that no Content Management System like WordPress, OpenCart, PrestaShop, Magento, Drupal, NopCommerce, etc., has any feature to protect customers' personal information from system admins. If viewing of personal data is granted to any system admin level, they can access, view, and download all the personal data of any specific or all users. There should be provisions that, except for top-level admin, others will be able to access limited personal data. As an example:

- *accountant does not need to watch the customer's phone number, email address, or date of birth,*
- *a sales agent really does not need to watch other sales agents' personal information, while the reality is, if a sales agent is given access to user data, they can see all users' personal information,*
- *the delivery person should know only the contact number and name of a person. He does not actually need to see the customer's email address, but when the delivery person hands over the open invoice, it shows everything from the email address to the payment method (if the payment was made online), which is unnecessary.*

Fraudulent activities can occur from any level of people who are connected to the e-Commerce service delivery. Therefore, if we could control access to personal data with the help of policy and technology, then we could keep our customers safer than at present.
I think, as the web platforms are developed, managed, and ruled by people and companies if the safety of personal data is assigned to the hands of people and companies, then it will never be possible to ensure the personal data safety of our customers. It can only be controlled if any eGovernance system can somehow control the personal data flow and access to the personal data."

Interview Dated: October 10, 2024

5.3. Case Study Findings

5.3.1. Case 1 Analysis

One of the interviewees shared an experience of personal data safety as follows:

"I am working as a software development team's Lead in a reputed company. Our product stakeholders from our company asked us about how we can protect personal data from our back-office Engineers like Database Developers, Database Managers, Software Developers, etc. To handle this situation, we created a system in our application/software where personal data is encrypted when it is stored in the database, so back-office engineers cannot read or misuse it. When we show this personal data on the web panels, only authorized users can access it. We would not allow our users to access reporting panels where we would see personal data that were presented on those report pages after decrypting from the database. Implementing this feature helped our stakeholders ensure that any back-office developers are not getting access to the personal data of customers and subscribers".

5.3.2. Case 2 Analysis

In an *interview* with a senior interviewee, some other essential features were found that can prevent data safety. Here is how he shared his experiences and knowledge:

"I am a senior web developer, and I lead a development team in a large software company. One of our client companies asked us for a feature that would allow their accounts department to view sales reports, order reports, transaction reports, etc., but they would not allow the accounts department to access an end-level customer's detailed information except the client's name or company name. We had to develop this feature for their custom as no modules/extensions were available for that platform to facilitate such provision. The client company also asked that the delivery people be able to access only a person's order details (except payment channel details), name, delivery address, and mobile number, but nothing else. We also developed a feature for them. From these requirements, we learned a good technological way of protecting personal data as per standard privacy policy".

6. OUTCOME OF THE RESEARCH

From the questionnaire, interview, and case studies, a set of essential outcomes are addressed, which are:

i. The collected data are from people of authentic sources who are deeply connected to technology management and are concerned about personal data safety [2.1.1].
ii. Any information of an individual or related to him is personal data, and people are frequently sharing such personal data on websites and software everyday [2.1.2].

iii. Personal data safety is a significant factor that people are also aware of [2.1.3].
iv. Loss of user data can lead to privacy, financial, reputation, and many other types of losses for a person [2.1.4].
v. Personal data might get lost due to not encrypting the data, allowing system/business users to access data openly, and not implementing any policy with the help of technology [2.1.5].
vi. Companies implement security to secure their websites or software from hacker attacks. However, in most cases, they do not take steps to protect personal data [2.1.6].
vii. By default, the Readymade Content Management System (CMS), which is commonly used by website developers to create E-Commerce and other business websites around the world, does not have any feature to protect users' personal information [2.1.7].
viii. Most of the website and software development companies do not maintain any globally accredited standard for personal data safety [2.1.8].
ix. The website and software development companies and their members have no sufficient awareness of personal data safety [2.1.9].
x. Industry technology experts suggest that companies should never allow engineers or business-people to access personal data from the panel or from a database level so that it can be preserved safely [2.1.10].
xi. The industry experts also suggest that, from company or individual level initiative personal data cannot be preserved safely, but with any government and policy level implementation, the government can keep personal data secure [2.1.11, 2.1.12]
xii. An industry expert has suggested the development of enterprise software and websites to such a standard that personal data cannot be accessed by system users who are not supposed to get these data [2.2.1].
xiii. Another industry expert suggested that instead of giving system users access to the personal data of all users, only certain personal information should be shown based on their particular request (such as finding a user's details using a User ID or getting transaction details using an Order ID). This would prevent system users from seeing large amounts of personal data with just one click. [2.2.2].

7. INTRODUCING A FRAMEWORK FOR PROTECTING PERSONAL DATA THAT ARE WIDELY USED OVER THE INTERNET

7.1. Establishing a Citizen Digital Identity Portal (CDIP)

The research says that only the government can control personal data safety. It is impossible to ensure personal data safety from the personal or company level as unethical parties might misuse the received personal data from their end users for their business or individual benefit. Therefore, only the government can establish a digital ecosystem that can protect personal data.

In any country, there is a specific ministry that has a database of its citizens in a digital format. Therefore, citizens' data already exists with the government digitally. This research proposes a Citizen Digital Identity Portal (CDIP), which will be connected to the citizen database (national identity information, birth registration information). This portal will create one single digital identity for each citizen. (Chart 17)

All the online stores will also be connected to this Citizen Digital Identity Portal (CDIP) so that they can verify a user with his/her digital identity.

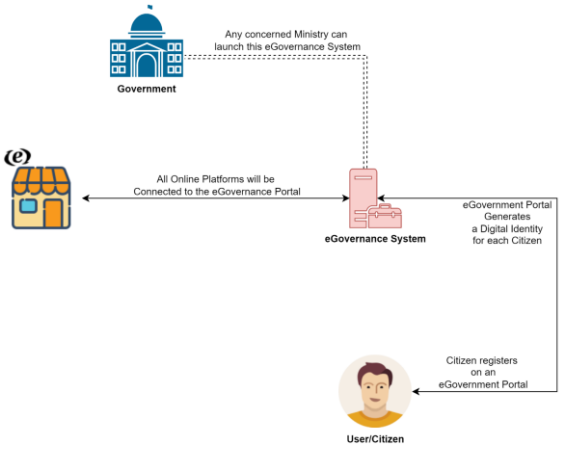

Figure Name: Chart 17

7.1.1. The Challenge of Establishing the CDIP:

It will not be very challenging to establish such an eGovernance Portal because to verify citizens and create an identity for them, the government would already and undoubtedly have a citizen database (national identity information, birth registration information) from before.

Creating and managing this kind of platform does cost a bit more, but it will help protect citizens' personal data and improve their safety from different types of risks. Hence, such kind of investment would not be a misuse or waste, but a valuable part of efforts to ensure the safety of citizens.

7.2. Data Safety at Company Level

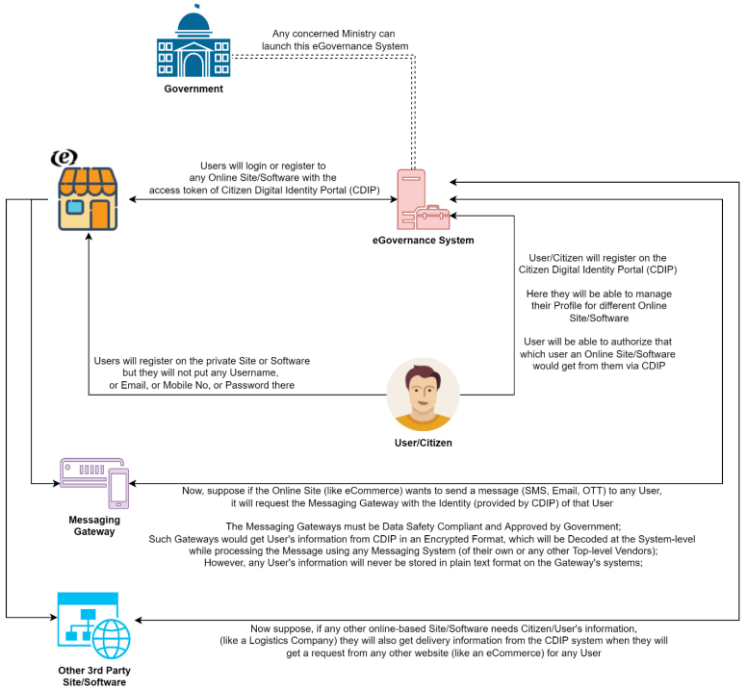

Figure Name: Chart 18

To secure Users'/Citizens' personal data over online platforms like websites or software, the platform owners would get connected to the CDIP eGovernance Portal API.

When a User wants to do any deal ('do register', 'do login', 'submit order', 'avail service', 'do transaction', 'get delivery') on any website, he/she does not require to put all types of personal information on the website. When the website requires any of the user's information, the website will simply request the CDIP eGovernance Portal, which will verify the user's information and inform the website about the verification status (whether the user's specific information is verified or not). In the very worst-case scenario, if the particular website (or any third-party website) needs any data, the CDIP API can send the data to the website in an encrypted form. There will be a CDIP package (a module) that the website has to use within the website that can decrypt the received personal data for processing. However, the CDIP package will help protect personal data on the website at the database or panel levels. There might be so many cases in how different personal data security can be ensured on the website/software; some major cases are explained below:

CASE 1 - User's registration on any Website:

- **Step 1:** Websites will use a CDIP-provided package, which will help the Website to synchronize the user's identity with the CDIP Portal.
- **Step 2:** The user registers on an eCommerce Website with his CDIP account.
- **Step 3:** CDIP provides an authentication token and an Identifier to the Website to validate the specific user.

RESULT: The user would not be required to provide his email address, username, or password to the website while registering online.

CASE 2 – Websites wants to send an Email to a User using its own SMTP Mailing Server:

- **Step 1:** Websites will use a CDIP-provided package, which will help the website synchronize the user's identity with the CDIP Portal. This CDIP-provided package will keep the user data encrypted on the website.
- **Step 2:** Now, to send an email to any user, the website will request the CDIP Portal to provide the user's email address.
- **Step 3:** The CDIP Portal will send the user's email address in an encrypted format, which the CDIP package will keep in an unreadable format at the database level and partially visible in the panel at the website level. Thus, the CDIP eGovernance ecosystem will ensure the safety of personal information.
- **Step 4:** The CDIP package will send the email address in plain text only to the SMTP Mailing Server as it delivers the email.

RESULT: Since most small-medium businesses and projects use their own SMTP mailing server to send emails (when using Shared Hosting), it becomes necessary to share the email address with these SME (or any other business) websites, as there is no other option. However, we can still protect the email address from unauthorized activities if we can implement the CDIP ecosystem.

CASE 3 – Websites want to send an SMS/OTT to a User using any 3rd Party's SMS/OTT Gateway:

- **Step 1:** Websites will use a CDIP-provided package, which will help the website synchronize the user's identity with the CDIP Portal. While the user registers on the website using a CDIP account, the website also receives a CDIP Identifier from the CDIP Portal.
- **Step 2:** Now, to send SMS/OTT to any user, the website will not request the CDIP Portal to provide the user's Mobile Number because it is the 3rd Party SMS/OTT Gateway that needs the Mobile Number, not the website. Therefore, the website will simply request the 3rd Party SMS/OTT Gateway to send an SMS/OTT to a CDIP Identity.
- **Step 3:** The 3rd Party SMS/OTT Gateway must be connected to the CDIP Portal, and from there, the Gateway will understand which mobile number would receive the SMS/OTT.
- **Step 4:** The SMS/OTT Gateway can also have the CDIP package to keep users'/citizens' personal information safe at the panel level or database level. After a formal compliance check-up, the government must approve Gateways, which carries millions of users' personal information.

RESULT: The gateway platforms, aggregator platforms, or top-level service vendor platforms can also ensure Personal Data Safety with the help of the CDIP ecosystem.

CASE 3 – Websites asks for the client's Address to send it to any 3rd party Delivery Company:

- **Step 1:** The websites will use a CDIP-provided package that will help the websites synchronize the user's identity with the CDIP Portal. While the user(s) do registration on a website using a CDIP account, the particular website will receive a CDIP Identifier from the CDIP Portal.
- **Step 2:** Traditionally, a website requires the delivery address of a user/customer so that they can provide it to any delivery company for delivering goods. Here, the website doesn't require receiving the delivery address, but rather, the delivery company would require this information as they will ultimately be delivering the product. Therefore, to inform a delivery company of the delivery address of any user/customer, the website will simply pass the CDIP Identifier of a customer to the delivery company.
- **Step 3:** The delivery company will get the delivery address from the CDIP Portal based on the received CDIP Identifier from any website (like an eCommerce Site).

RESULT: This process will restrict websites (like eCommerce Sites) from not getting the delivery address of a user/customer; however, only the delivery companies will receive it.
In many cases where SME websites (small-scale eCommerce businesses) deliver their products by themselves, they would get delivery information of their customer directly from the CDIP.

CASE 4 – Websites ask for and saves the Shipping/Billing Address of any customer in a case while the Website itself delivers the product:

- **Step 1:** The website will request the user/customer's shipping/billing address for service delivery purposes on their platform, and in such cases, the website will use a CDIP-provided package to synchronize the user's address from the CDIP Portal. This CDIP-provided package will keep the User Data encrypted on the website.
- **Step 2:** The CDIP Portal will provide the user's shipping/billing address in an encrypted format, which the CDIP package will maintain in an unreadable format at the Database level and partially visible at the Panel level on the website.

RESULT: In many cases, online websites also handle the delivery of their goods with their own teams, leaving no alternative but to store shipping/billing addresses on the website. However, the CDIP package will ensure that the data remains encrypted in the database and partially visible in the panel, thereby ensuring personal data safety within the CDIP eGovernance ecosystem.

CASE 5 – Websites ask for and save NID (National ID) No, Passport No, etc. from the customer for verification purposes:

- **Step 1:** Some websites request NID numbers, passport numbers, and similar personal information to verify a customer's identity. In such cases, the website does not need to collect this personal data; instead, it is sufficient for the CDIP Portal to hold this information.
- **Step 2:** When a website needs to verify a person's NID number, passport number, driver's license number, or similar information, the CDIP API will simply confirm that the individual has already verified their NID number, passport, driver's license number, or other similar information through the CDIP Portal. Based on the confirmation from the CDIP Portal API, the website will proceed to verify the user.

RESULT: The CDIP eGovernance ecosystem can verify a person's information and send a verification token to websites that need to confirm a person's identity. Thus, the websites would not need to collect citizens' information at all.

7.2.1. Data Safety Hassle at Company Level

Connectivity with an eGovernance Portal (CDIP) via API is not a significant or expensive factor for any website or software. Moreover, this will ensure the security of personal data for users/citizens on all websites/software and their third-party platforms as well.

At the initial stage, it may be challenging for any government to implement this ecosystem nationwide. Therefore, in the first phase, the government may begin by providing a seal/badge to websites/software that are CDIP Compliant to ensure Personal Data Safety. This will raise awareness among users/citizens, prompting them to be cautious when providing information on any CDIP non-compliant website/software. Later, in the subsequent phase, the government may require all websites/software to connect to the CDIP ecosystem to ensure Personal Data Safety.

7.2.2. Benefit to the Companies in Getting Integrated with CDIP

When a website remains connected to the CDIP eGovernance Portal, it will be safe for the website owners as well. As the CDIP Portal ensures identity verification for the websites (such as: email verification, NID verification, Passport verification, and phone number verification), it will help the website owners avoid fraudulent orders and transactions.

Moreover, when the CDIP eGovernance Portal provides a seal/badge to the website or software indicating "this website/software is CDIP verified," it will also enhance the platform's brand value. Customers will feel more secure engaging with the website/software.

8. FUTURE WORK

As personal data safety for all citizens in a country is a massive project, it is not a small research endeavor. This paper aims to present the best possible set of solutions to protect the most common personal information that is frequently shared on online websites and software.

There is some additional personal information that could not be addressed in this paper; therefore, a solution to personal data safety for all kinds of personal information could not be covered in this paper.

Moreover, even though the ideas in this paper can be used in any country worldwide, there may still be some limitations that could be solved if the research included data from all other continents.

More work can be done to improve the framework so that it protects all types of personal information without hurting businesses or causing high costs.
This paper did not address cross-border business scopes; therefore, it does not consider what would happen when a website's users are from multiple countries. Further research on this topic will cover this scope as well.

9. CONCLUSION

Providing security for private data being transmitted on public and private digital networks is one of the most challenging issues in today's cyber world. This study offers a broad framework that governments and different private organizations can use to protect private data from being misused, accessed without permission, or targeted by cyber-attacks. Through the incorporation of encryption, access controls, and API-based identity verification, the suggested Citizen Digital Identity Portal (CDIP) provides a cost-efficient, scalable, and policy-based approach to reducing risks in current personal data management procedures.

Founded upon detailed industry surveys, interviews with professionals, and actual case studies, the study identifies key personal data protection deficiencies, including lax regulatory enforcement, lack of consistent security policies, and weak technical protections. Studies indicate that businesses cannot entirely ensure data security on their own, so there is a need for a centralized, government-backed initiative introducing stringent security controls and compliance practices.

The adoption of this framework will bring long term value. It will not only make cybersecurity stronger and support data privacy laws, but it will also help businesses and software platforms by providing a secure, government-approved authentication process. This will deter identity fraud, enhance digital trust, and simplify identity verification processes, ultimately creating a safer digital environment for users and businesses.

Although this study constitutes the basis for a sound and ordered method of personal data security, additional efforts are necessary in developing its extension to cross-border electronic transactions, multi-industry convergences, and future cybersecurity threats. With digitalization picking up speed, governments and institutions have the responsibility to implement personal data security to enable citizens to utilize online platforms without compromising their security and privacy.

By bridging the gap between cybersecurity policy and technology, this research helps towards a sustainable and future proof framework which can pave the way for more stringent data protection policies and more secure digital infrastructures in the coming years.

CONFLICT OF INTERESTS

The authors declare no conflict of interest.

REFERENCES

[1] A. Uberoi, “Top 10 biggest cyber attacks of 2024 & 25 other attacks to know about!,” Cm-Alliance.com, 2024. [Online]. Available: https://www.cm-alliance.com/cybersecurity-blog/top-10-biggest-cyber-attacks-of-2024-25-other-attacks-to-know-about.

[2] J. Brustein, “RadioShack’s bankruptcy could give your customer data to the highest bidder,” Bloomberg, Mar. 24, 2015. [Online]. Available: https://www.bloomberg.com/news/articles/2015-03-24/radioshack-s-bankruptcy-could-give-your-customer-data-to-the-highest-bidder.

[3] A. Carbone and J. Kaasbøll, “A survey of methods used to evaluate computer science teaching,” in Proc. 3rd Annu. Conf. Integrating Technol. Comput. Sci. Educ., Aug. 1, 1998. [Online]. Available: https://doi.org/10.1145/282991.283014.

[4] United Nations Conference on Trade and Development, “Data protection and privacy legislation worldwide,” UNCTAD, Apr. 2, 2020. [Online]. Available: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

[5] S. Demeyer, “Research methods in computer science,” in Proc. 2011 27th IEEE Int. Conf. Softw. Maint. (ICSM), 2011. [Online]. Available: https://doi.org/10.1109/icsm.2011.6080841.

[6] S. Gibbs, “Ashley Madison condemns attack as experts say hacked database is real,” The Guardian, Aug. 19, 2015. [Online]. Available: https://www.theguardian.com/technology/2015/aug/19/ashley-madisons-hacked-customer-files-posted-online-as-threatened-say-reports.

[7] G. Greenwald, “NSA collecting phone records of millions of Verizon customers daily,” The Guardian, Jun. 6, 2013. [Online]. Available: https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

[8] B. Krebs, “Online cheating site Ashley Madison hacked,” Krebs on Security, Jul. 15, 2015. [Online]. Available: https://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/.

[9] R. McMillan, “Yahoo says information on at least 500 million user accounts was stolen,” Wall Street Journal, Sep. 23, 2016. [Online]. Available: https://www.wsj.com/articles/yahoo-says-information-on-at-least-500-million-user-accounts-is-stolen-1474569637.

[10] E. Nakashima, “Hacks of OPM databases compromised 22.1 million people, federal authorities say,” The Washington Post, Jul. 9, 2015. [Online]. Available: https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/.

[11] PrivacyPolicies.com, “What’s data privacy law in your country?”, Privacy Policies, Sep. 4, 2019. [Online]. Available: https://www.privacypolicies.com/blog/privacy-law-by-country/.

[12] S. Alder, “UHG: Substantial Proportion of US Population May Be Affected by Change Healthcare Cyberattack,” *HIPAA Journal*, 2024. Available: https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/.

[13] T. Ambrose, “UK armed forces’ personal data hacked in MoD breach,” *The Guardian*, May 07, 2024. Available: https://www.theguardian.com/technology/article/2024/may/06/uk-military-personnels-data-hacked-in-mod-payroll-breach

[14] Nguyen Hong Son and Ha Thanh Dung, "A Lightweight Method for Detecting Cyber Attacks in High-Traffic Large Networks Based on Clustering Techniques," *International Journal of Computer Networks & Communications (IJCNC)*, vol. 15, no. 1, pp. 35–51, Jan. 2023. doi:10.5121/ijcnc.2023.15103.

AUTHORS

Nirjhor Anjum is a cybersecurity expert, eGovernance strategist, and digital services specialist with a strong academic and industry background. As a National Cybersecurity Consultant for Ministry of Planning (BD), he contributed to the eGovernance projects. As an Assistant Professor at DIU and active researcher, he has contributed to cybersecurity, AI-driven automation, and software engineering through peer-reviewed publications. He has taught more than 2,300 students as an academician. In executive roles in the IT industry as CTO, CBO, and CAO, he led Cybersecurity, eGovernance, FinTech, Enterprise Automation, Business Intelligence, and various other enterprise digital transformation projects. With expertise in large-scale IT infrastructures, SaaS solutions, and public-sector digitalization, he is a thought leader connecting research with real-world innovation.

Lamia Islam is an Assistant Professor of Political Science at Jagannath University (JnU), Bangladesh, specializing in e-Governance, governance, conflict resolution, peacebuilding, and migration studies. A Ph.D. candidate at Washington State University, her research focuses on political participation, gender dynamics, and forced migration. Her 2024 Gender Issues article, "Patriarchal Masculinities and Cyberbullying on Facebook," examines digital violence as a governance and human rights issue in Bangladesh. As a Lovrich Research Fund Fellow (2024-2025), she is studying female students' political participation and gender equality in higher education. She has worked with UK Aid, IFES, and the Centre for Genocide Studies on Rohingya displacement, election monitoring, and political violence, contributing to debates on governance, peace-building, and digital security.

Md Rubel Chowdhury is a researcher at London Metropolitan University (SCDM), UK, specializing in computer networking, cybersecurity, and web development. He is pursuing an M.Sc. in Computer Networking and Cyber Security, with 3+ years of IT experience in roles at Foster Technologies, SuperbNexus, and XoomServer, and received Rising Star Award 2021. His expertise includes Vulnerability Assessment, Cloud Server Management, PHP development, CMS management, QA, Laravel, OpenCart, etc. A top graduate with the highest CGPA of 3.92 from Bangladesh University, he ranked 2nd in merit. His work focuses on web security and digital infrastructure resilience.

Ariful Alam is pursuing Doctor of Information Technology specializing in Cybersecurity at Trine University, USA. He holds an M.Sc. in Information Technology from Washington University of Science and Technology and a B.Sc. in Electrical and Electronics Engineering from Leading University, Bangladesh. A certified Scrum Master and Product Owner, he has led IT projects across software, web, and mobile development. His expertise includes Agile methodologies, JIRA administration, technical documentation, and cybersecurity. Ariful has also published research on hexacopter systems and actively contributes to technology and robotics initiatives.