Acknowledgments

I am grateful to **Allah Almighty**, the benevolent, merciful, and generous. His glory and countless blessings nourished my aspirations and goals; blessed me with excellent instructors, loving parents, and kind siblings.

I convey wholehearted thanks and a deep sense of gratitude to my respected **Supervisor Dr Adnan Noor Mian**, Department of Computer Sciences, Information Technology University, Lahore, Pakistan. His expert advice, the art of making valuable and worthy suggestions, unfailing patience helped me a lot throughout the research work. I would also like to thank the **Dedicated team** under his supervision that has always put useful insights into my work.

I extend my feeling of gratitude and indebtedness to my **beloved mother** who always supported and motivated me in every field of my life. I express heartiest thanks to my beloved and honorable sister **Ms. Ayesha Raana**, Department of Computer Science, GC Women University, Sialkot, Pakistan. She is a true guider, who always guided me to the right path to move upon and always been a great motivation.

Last but not the least, I pay cordial obligations, good wishes, and inspirations to my **family members, well wishers and the friends** who are there for me with their kind prayers.

Table of Contents

List of Figures

List of Tables

Abstract

Workplace harassment and discrimination are prevalent issues that have a detrimental effect on a victim's working environment. Every state or country has its own system of regulations that apply to workplace harassment cases. Given such regulations from Pakistan, the objective of this work is to propose an Ethereum-based dApp that carefully adheres to the legislative law, i.e., the protection against harassment of women at workplace Act **(PAHWAWA 2010)** while protecting females' rights to respect and decency.

Even though the government of Pakistan has enacted legislation (PAHWAWA 2010) over the past decade, workplace harassment of females is still on the rise. According to different case studies, the current procedure for enquiring about harassment complaints at workplaces is not effective enough to ensure justice as per the law. The higher authorities try to consider the company's reputation first, and such a trend is normalising the harassment. To the best of our knowledge, there is no such system that strictly implements the legislated law, i.e., PAHWAWA 2010.

The goal of the proposed work is to develop a tamper resistant and decentralized platform for female employees to register harassment accusations. Women at the workplace can file complaints via a secure application with the assurance that their data cannot be tampered and no higher authority can compel them to withdraw their complaints. According to the annual statistics by Federal Ombudsman Secretariate for Protection Against Harassment (FOSPAH), government of Pakistan , workplace harassment incidents are increasing at an alarming rate. The reason for this rising trend is that the legislation PAHWAWA 2010, has not been strictly enforced in the various organizations.

The strict implementation of this law (via Ethereum dApp) will ensure that the accused has received the appropriate punishment under the law, and it will eventually put an end to the workplace harassment trend. Furthermore, the proposed system will make sure that more female victims are coming forward and filing complaints against any harassers since the system promotes trust and confidence in its users because no one will be able to withdraw or change the complaint. In any case, if the victim feels that the decision of the inquiry committee is unjustified, she may pursue retaliation by filing a lawsuit against both the accused and the organization. The success of the system will be determined by testing its performance, i.e., ensuring that the legislation is enforced strictly, assessing cost and time metrics, and evaluating the system's effectiveness in a real-world scenario.

Chapter 1
Introduction

This chapter defines harassment, workplace harassment, the traditional process of filing harassment complaints in Pakistan, motivation towards this area of study, and research questions in the subject matter. The chapter highlights the problem statement, the research objectives, as well as limitations and scope of the current work. This chapter concludes its findings by addressing the problem statements of this work.

1.1 Overview

Harassment and Sexual violence are usually characterized under statutory regulations that differ with jurisdiction for different states. However, it is frequently defined as an action that frustrates, annoys, or forces an individual to feel uncertain about his/her security. Harassment can occur in many forms. One such form is sexual harassment. Sexual harassment is considered to be unscrupulous conduct that is combative and intrusive. It could be considered as an oral/ or non-oral victimization with an unethical demeanor to force someone for an unwanted sexual relationship or sexual intimidation i.e., blackmailing, bribery and threatening.

Workplace harassment has turned into one of the serious and contentious issues of the twenty-first century, contributing to the psychotic breakdown of female employees. This predicament in East Asia is far more ominous and is also one of the challenges that organizations have failed to address. According to studies, workplace harassment not only demoralizes female employees but also affects their work effectiveness, which ultimately leads to long-term physiological repercussions.

Furthermore, it is incredibly challenging for the victims of sexual harassment to come forward and file a case or make a statement about what happened. This option becomes far more stressful if it occurs at workplace, as there will be countless other factors that may influence the decision to raise this concern. It can have a substantial impact on a victim's emotional well-being, along with forcing them to switch jobs, contribute to unemployment, and possibly result in the loss of well-paying jobs. Despite the fact that the consequences are miserable, many victims opt not to disclose the assaults to their respective workplaces. Furthermore, victims who opt to file a complaint bear the uncertainty of nothing being done.

Ganga Vijayasiri investigated the impact of the organizational environment on victims' willingness to pursue sexual harassment allegations, including victims' fear for retaliation, lack of confidence in the system, and anxiety of being criticized or ridiculed before the society. One of the barriers to reporting, according to the study, is the fear of unfavorable repercussions that includes its negative impact on the victim's career or fear of being scapegoated for the incident. According to the same

survey, half of the victims reported that nothing has been done about their complaints, which is not surprising given that most complaints are usually withdrawn from higher authorities for the sake of the company's reputation and image in society [1].

In Pakistan, this problem is not unique. Pakistani female employees encounter workplace stress and harassment repeatedly on daily basis. Females ought to work with males to balance the financial load for their households to function well. However, due to the lack of institutional support and protection, speaking up against workplace harassment is still deemed inappropriate for females in the patriarchal social system in Pakistan.

It is essential to sustain a secure, fair, and harassment-free working climate for employees to be more motivated, efficient, and passionate while achieving maximum outcomes. Victims must be given considerable assistance, equal protection under the law and access to justice to not only compensate for what occurred, but also to prevent such conducts from happening again in the working place. Certain States, including Pakistan, have enacted legislation addressing employers' and employees' legal obligations and rights to encourage a harassment-free working environment. Organizations are legally obligated to incorporate legal interventions for preventing harassment and discrimination at the workplace. Figure 1.1 illustrates the formal procedure of how a harassment complaint looks like while considering the Pakistani legislation against workplace harassment (Act No. IV of 2010 - Protection against Harassment of women at the Workplace Act, 2010) [2].

According to the Act **(Act No. IV of 2010 - Protection against Harassment of women at the Workplace Act, 2010)**, **Harassment** is defined as *"any unwelcome sexual advance, request for sexual favors or other verbal or written communication or physical conduct of a sexual nature or sexually demeaning attitudes, causing interference with work performance or creating an intimidating, hostile or offensive work environment, or the attempt to punish the complainant for refusal to comply to such a request or is made a condition for employment"* [2]. However, a victim has an open choice to proceed with the complaint either by choosing an Ombudsman or an Inquiry Committee.

The Ombudsman is a legal authority appointed by respective Government at the Provincial or Federal levels to investigate such cases. Every organization is obliged to form an Investigation Panel of three members (a woman, a senior manager, and a senior representative of employees) to investigate complaints made under this Act. In case the perpetrator is a part of this committee, it is mandatory to replace it with some senior investigator (within or outside the organization). Furthermore, the organization is required to appoint a Competent Authority to impose a major or minor penalty (as specified in the Act) on the accused within one week of the Inquiry Committee's decisions and recommendations [2]. Figure 1.2 depicts the possible entities that may be involved in the complaint procedure as required by applicable Law [2].

Even though the Government of Pakistan (GoP) has enacted legislation (Act IV of 2010) to promote citizens' rights to respect and decency over the past ten years, workplace harassment is still on the rising trend [2]. Organizations are unable to strictly enforce the law and fail to provide female employees

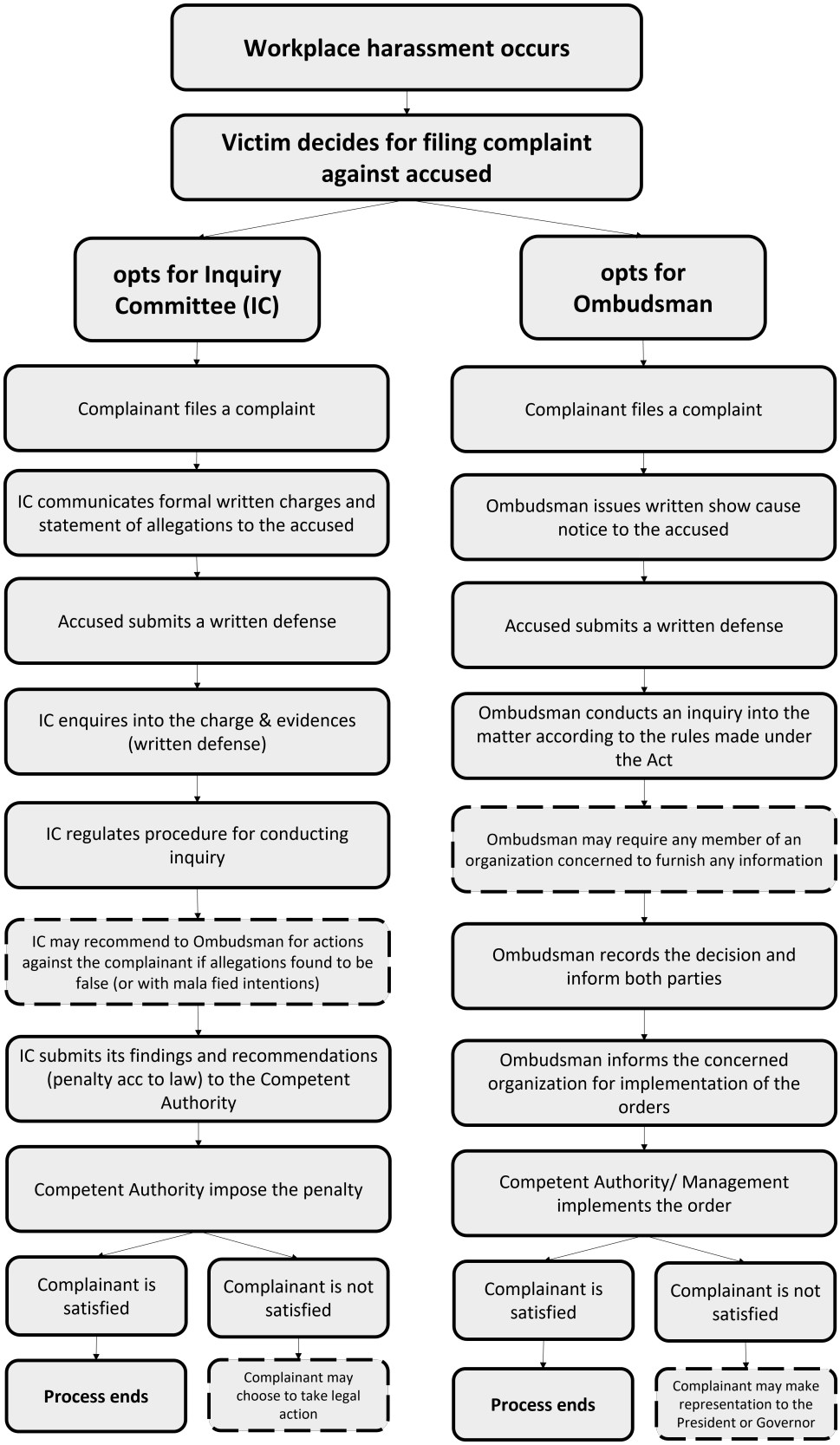

Figure 1.1: Harassment Complaint Process as legislated by GoP, Act IV of 2010.

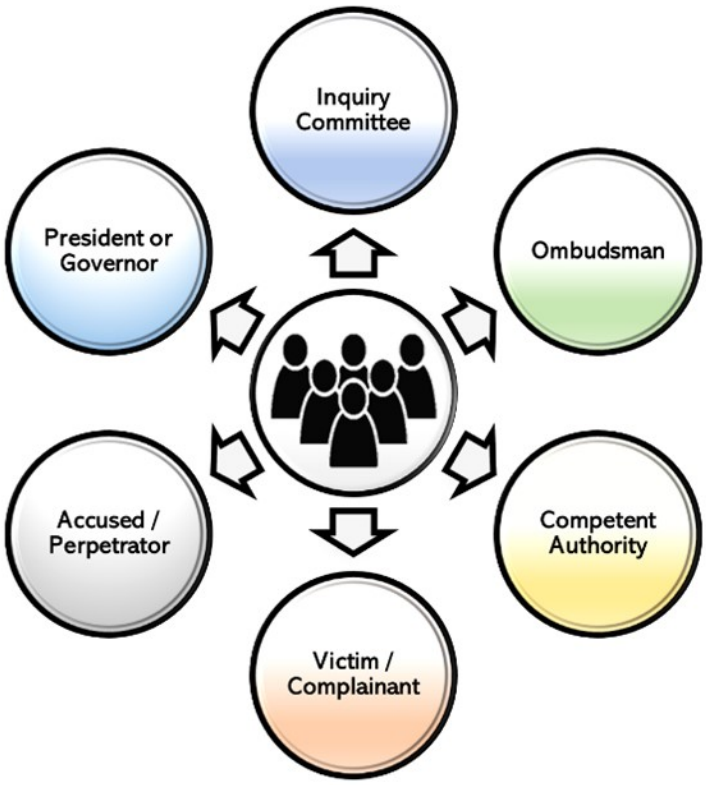

Figure 1.2: Users in Harassment Complaint Process - as legislated by GoP, Act IV of 2010.

with enough safety and security. Discrimination and harassment at the workplace are becoming one of the most significant barriers especially for females willing to join the professional workplaces in Pakistan. Considering such serious concerns, there is a dire need for a decentralized and trust-free platform that exactly maps and strictly follows the legislated law from GoP *[Act No. IV of 2010 - Protection against Harassment of women at the Workplace Act, 2010]* to guarantee a safe and secure environment for sexually harassed victims while preventing such incidents from happening again in the future [2].

1.2 Problem Statement

Workplace harassment and discrimination at the workplace is considered to be a pervasive issue, with a devastating toll that affects the working environment of a victim; negatively influencing the employee's job performance and well-being. Many companies still have a knee-jerk reaction to harassment complaints because they see it as a waste of time and resources that would end up hurting the company's reputation in the public's eye. Even though the Government of Pakistan has implemented legislation (Act IV of 2010) to promote citizens' rights to respect and decency over the past ten years,

workplace harassment is still on the rising trend [2]. Organizations are unable to strictly enforce the law and fail to provide female employees with enough safety and security. Being a patriarchal society, it is difficult for female victims in Pakistan to speak out against what has happened to them because it disregards their dignity and respect in society. If any of the victims file a complaint, they generally do not receive a satisfactory response from higher authorities, which eventually normalizes harassment and forces the victims to change workplaces. Considering this situation, there is a dire need for a decentralized and trust-free system for victims to file a harassment complaint that strictly follows and implements Pakistani law (Act IV of 2010) to not only promote a safe and conducive work environment for female employees, but also to prevent such cases from occurring in the future [2].

1.3 Objectives

The current study will answer the following research questions while considering the traumatic condition of workplace harassment in Pakistan.

1. **What could be a feasible trust-free framework for such system effectively supporting workplace harassment complaint processes?**

   A blockchain-based system could be helpful in this regard that should provide a decentralized and trust-free platform for victims to file such complaints. The complaint system should be decentralized, such that no higher authorities have the right to withdraw any complaint- for the sake of their company's reputation.

2. **How will the concerned system empower female employees to file such complaints?**

   The Blockchain-based system will ensure ***anonymity and confidentiality*** *to all information provided by victims i.e., no data will be shared with unauthorized persons; in order to preserve their privacy without jeopardizing their image and reputation in society.*

3. **How will the concerned system prevent such cases to happen in the workplace again?**

   The concerned system will ensure that the relevant law (Act IV of 2010) [2] is judiciously followed, while also guaranteeing that the harasser has been penalized/ punished rigorously according to law, which would ultimately reduce recurrence of similar cases in future.

4. **How will the concerned system prevent registering fake complaints?**

   The concerned system will involve the ***Department of Forensics****, which will make sure that all the documents and evidence shared by any of the arty have not been tampered with. The blockchain system will only store those documents which will be verified by the Department of Forensics i.e., no fake pieces of evidence will be entertained.*

The proposed Blockchain based harassment complaint system will allow the victim and all the stakeholders to keep the record of the submitted complaint until it is resolved. It'll ensure the victim that nobody has the authority to withdraw the complaint. To ensure the credibility of filed complaints, the system will make sure to verify the provided pieces of evidence, and all the documents from both the parties before investigating it and storing it in Blockchain. No fake complaint will be registered in this process and the system will make sure that the harasser in any case pays the penalty decided by the law. It will enable the victim to retrieve all the documents (with time stamps) and pursue legal actions if he/she is not satisfied with the inquiry results. The system will make sure that victim get justice according to Pakistani law. It'll not only compensate for what happened to the victim but also help in preventing such situation to happen again.

1.4 Limitations and Scope

The current study aims to enable the adoption of a decentralized framework i.e., a blockchain solution for controlling and preventing workplace harassment. The study presents a decentralized and trust-free system to facilitate every organization in reporting harassment reports. The main objective is to **limit workplace harassment** while concentrating on the fact that there should not be any central entity to register such complaints. For the sake of the company's reputation, the complaint file system should not be able to delete or withdraw any complaint.

The proposed system takes into account all of the users specified in Act IV and strictly follows and implements Pakistani legislation [2] enacted specifically for this concern. Moreover, in order **to avoid the filing of fake harassment complaints**, a new entity *(Department of Computer Forensics)* has been introduced to this system for the purpose of verifying all digital documents. The smart contracts used for this purpose will be able to maintain track of all transactions from authorized parties, timestamping them and ensuring that no one has the authority to tamper with or withdraw any document or information.

In addition, the current study will present thorough security and cost analysis to evaluate the performance of smart contracts in terms of ensuring the feasibility of the proposed system.

However, the smart contracts for the solution are implemented and deployed using Remix platform; an Ethereum based framework. However, testing and deploying the system in a real environment is currently challenging due to a lack of computing resources. To address this shortcoming, the current work strongly recommends the deployment of a proposed system in real-world context to evaluate its performance.

1.5 Thesis Outline

The remaining content and report is arranged in such a way that Chapter 2 provides a detailed background study and literature review pertinent to this problem. Chapter 3 presents the proposed system i.e., architecture and flowchart. The complete experimental setup, metrics, findings, and discussion regarding the proposed approach are outlined in Chapter 4 . Finally, in Chapter 5, the study comes to an end.

Chapter 2
Literature Review

The current chapter summarizes the related work and the existing literature relevant to the stated problem. However, there is currently no literature published so far on this specific problem.Therefore, this study has explored the relevant applications and context wherein blockchain technology has already been employed. The following sections briefly highlight the Consequences and Antecedents to workplace harassment, Complaint procedures and policies, major findings of Pakistani Act No. IV against harassment at workplaces, and state of the art solutions for dealing with harassment. Moreover, the existing literature includes different applications of blockchain in Human Resource Management, Combating digital deception using blockchain, and Smart Voting and Record Management. This chapter concludes with investigating the interconnection between Computer Sciences and Law; presenting Blockchain and its legal Implications.

2.1 Related work

This section highlights related work that is relevant to the current study. It illustrates the effects and antecedents of Workplace Harassment as revealed differently by different researchers in the field. The findings demonstrate the different types of complaint procedures and policies, and the major findings of Pakistani Act No. IV enacted by the Government of Pakistan against workplace harassment. The related work also highlighted the most recent state-of-the-art strategies for coping with harassment. The debate that follows supports the notion of proposing a complaint system to deal with such a traumatic increase in workplace harassment.

2.1.1 Consequences and Antecedents to workplace harassment

Workplace harassment and violence have been among the social and controversial issues in the twenty-first century, contributing to the psychological breakdown of women employees. This predicament in East Asia is far more ominous and is also one of the challenges that organizations have failed to address [3].

In Pakistan, this problem is not unique. Pakistani female employees encounter workplace stress and harassment repeatedly on daily basis[4]. Females ought to work with males to balance the financial load for their households to function well. However, due to the lack of institutional support and protection, speaking up against workplace harassment is still deemed inappropriate for females in the patriarchal social system in Pakistan [5].

Considering this traumatic situation, the Government of Pakistan legislated an act [Act No. IV OF

2010] to promote female's rights at workplace and to provide them legal support and protection. This Law is premised on the idea of providing female employees with equal rights and establishing a safe and healthy work environment for them [2].

Yasmin and Sadia came up with a study in Pakistan, revealing that despite of this legislation, the female victims still avoid filing the complaint against the perpetrator The study revealed the potential concerns for women avoiding reporting workplace harassment in Pakistan. According to them, in Pakistani society, women's modesty, the anxiety of being humiliated, or loss of employment have been the most common concerns for not reporting sexual harassment in the workplace [6]. Sadruddin (2019) showed several studies that verified this argument, revealing that the majority of women believe that reporting harassment is similar to losing a job because the inquiry committee did nothing for the sake of company's reputation. Furthermore, reporting an incident of sexual misconduct ultimately put a spotlight on the victim's reputation results in unbearable cost in terms of job insecurity, the criticism of society, and constant fear of retaliation [7].

A study by Nighat Yasmin (2018) in Lahore Pakistan also revealed some realities to this situation in which female victims avoid consulting these incidents with families. And when it comes to reporting, they prefer to report vocally rather than in-writing. They exclusively report to the company management, not to other concerned authorities i.e., the law department or ombudsman. The study ended up finding that perpetrators of sexual harassment are not prosecuted and punished in accordance with the law. The authorities simply make sure that perpetrators have apologized to the victim or are officially warned. And such minor penalties are questionable in the light of such a situation that seems to be deteriorating by the day [6].

Many companies are still using paper-based complaint forms for recording and filing harassment cases at workplace; some have their very own self-developed centralized complaint management tools, while others use third-party software. It might be challenging for the victims of workplace harassment to rely on the system being under the supervision of the company's manager or owner. Therefore, there is a dire need to come up with a solution that should not be centralized i.e., that should provide immutability and confidentiality to victims' data taking into account Pakistani legislation in this respect.

2.1.2 Harassment Complaint procedures and policies

The policies for workplace harassment and complaint procedures differ from one organization to the next; distinct in every jurisdiction based on regional regulations. Such policies are often classified as formal or informal. According to Feldman-Summers, a formal procedure for filing a harassment complaint is one in which the victim is obligated to register a written statement, which is accompanied by some kind of formal inquiry. A thorough investigation is done to carry out the necessary inquiry, which ultimately results in punishment for the perpetrator if accused of a crime. Moreover, informal

procedures primarily include oral reports to senior management preceded with a less formalized inquiry to figure out a solution, without the need for a verdict of abuse or even a penalty for the alleged perpetrator [8].
According to Velázquez and Jain, sometimes communicating explicitly to the perpetrator that "such action is not acceptable, intimidating, causing the victim queasy, and affecting the victim's productivity" could be adequate to address such situation informally. However, the researchers also emphasize the fact that there are certain situations in which informal approaches to reconcile or negotiate should never be employed. That'll be applicable for situations that have intensified to the point where coming to an agreement is impossible, or because the claimed acts are unjustified. Therefore, the study recommends a formal approach in certain circumstances when the informal one fails to settle the matter. It may consider registering a documented and formal complaint through particular channels, notifying the accused perpetrator, and conducting an internal inquiry by an independent authority within a timeframe. The investigation report then must also be made available to the employer. However, all the sensitive and personal information of individuals/victims must be kept confidential throughout the process [9].

2.1.2.1 Harassment Complaint Procedure in Pakistan- ACT IV of 2010

Considering the devastating increase in workplace harassment, the constitution of the Islamic Republic of Pakistan also acknowledges citizens' basic rights and enacted an act ***[Act No. IV of 2010 - Protection against Harassment of women at the Workplace Act, 2010]*** to guarantee security and safety for females in the working environment [2]. Moreover, any victim of workplace harassment has an open choice to either choose for an Ombudsman or an Inquiry Committee established especially for this purpose, as per the respective law. The major findings of this act are as follows:

(a) **Inquiry Committee to enquire into complaint**

1. Each organization (Workplace) shall constitute an Inquiry Committee within thirty days of the enactment of this Act to enquire into complaints under this Act.

2. The Inquiry Committee, within three days of receipt of a written complaint, shall–

    - communicate to the accused the charges and statement of allegations levelled against him, the formal written receipt of which will be given;
    - require the accused within seven days from the day the charge is communicated to him to submit a written defense and on his failure to do so without reasonable cause, the Committee shall proceed ex-parte; and

- enquire into the charge and may examine such oral or documentary evidence in support of the charge or in defense of the accused as the Committee may consider necessary and each party shall be entitled to cross-examine the witnesses against him.

3. Inquiry Committee shall have the power to regulate its own procedure for conducting the inquiry and for the fixing place and time of its sitting.

4. The following provisions inter alia shall be followed by the Committee in relation to inquiry:

    - The statements and other evidence acquired in the inquiry process shall be considered confidential.
    - Adverse action shall not be taken against the complainant or the witnesses.
    - The Inquiry Committee shall ensure that the employer or accused shall in no case create any hostile environment for the complainant to pressurize her from freely pursuing her complaint; and
    - The Inquiry Committee shall give its findings in writing by recording reasons thereof.

5. The Inquiry Committee shall submit its findings and recommendations to the Competent Authority (within thirty days of the initiation of inquiry.

6. If the Inquiry Committee finds the accused to be guilty it shall recommend to the Competent Authority for imposing one or more of the mentioned penalties

7. The Inquiry Committee can instruct to treat the proceedings confidential.

(b) **Ombudsman to enquire into complaint**

1. The respective Governments shall appoint an ombudsman at the Federal and provincial levels.

2. The Ombudsman shall within 3 days of receiving a complaint issue a written show cause notice to the accused.

    - The accused after the receipt of written notice, shall submit written defense to the Ombudsman within five days and his failure to do so without reasonable cause the Ombudsman may proceed ex parte.

3. The Ombudsman shall conduct an inquiry into the matter according to the rules made under this Act and conduct proceedings as the Ombudsman deems proper.

4. For the purposes of an investigation under this Act, the Ombudsman may require any office or member of an organization concerned to furnish any information or to produce any document which in the opinion of the Ombudsman is relevant and helpful in the conduct of the investigation.

5. The Ombudsman shall record his decision and inform both parties and the management of the concerned organization for implementation of the orders

(c) **Representation to President or Governor**

Any person aggrieved by a decision of Ombudsman may, within thirty days of decision, make a representation to the President or Governor, as the case may be, who may pass such order thereon as he may deem fit [2].

Following the passage of even more than one decade, workplace harassment is still challenging and controversial in Pakistan due to the lax enforcement of the legislated act. There is a dire need for a system that should strictly adhere to the legislation for preventing harassment at workplaces. As per the knowledge of this study, there is no such promising system that should map and implement the Pakistani law to deal with such a traumatic situation.

Considering the antecedents and consequences, the study proposes the adoption of a blockchain-based platform to introduce a harassment complaint file system. There is no such system reported in the literature so far; however, there are certain studies that are supporting the use of blockchain for this problem. The literature review in Section 2.2 summarizes existing applications that have been using blockchain-based solutions for autonomous and decentralized systems.

2.1.3 Combating harassment: State-of-the-art solutions

Hyo Jin Do and co-researchers have proposed a proof-of-concept design for a Conversational Interface; could be employed in Harassment Awareness Program. This interactive chat session includes a harassment vignette, i.e., a personal story that imitates how a victim might discuss any harassment incident in person. The user takes on the role of a listener; participates in a constructive conversation to offer advice and sympathy to the victim. It will ultimately encourage the listener to explore preventative measures while giving suggestions to the victim on how to deal with this scenario. different questions in the interactive session will encourage the listener to think about real-life harassment events at their workplace. Since most participants are uncomfortable discussing such matters in person, the researchers believe that such interactive platforms might play a significant role in Sexual Harassment training [10].

Shiri Sadeh-Sharvit and his co-authors have presented a contemporary virtual reality solution for training or providing countermeasures for controlling workplace harassment. They did a proof-of-concept analysis to see whether a virtual interview process may be an effective learning strategy for females and could serve as the foundation for developing improved response skills. A virtual environment of such a type mimics a virtual job interview session wherein a semi-automated virtual operator functions as an interviewer and sexually abuses the interviewee. The findings imply that such contemporary virtual characters in augmented reality may communicate a perception of being

harassed. And such a virtual reality platform can provide a safe setting for women to experience sexual harassment; that could be beneficial as a training guide [11]
Nabila Rezwana Mirza and her collaborators have proposed a portable defensive device i.e., a sensor support to deal with sexual harassment. The mini device is Bluetooth-enabled and has a touch-pad sensor; linked to a software application on the user's phone. This small device acts as a trigger; maybe hidden anywhere, such as in a purse or clutch. Bluetooth connection prompts the application to send a HELP message to the listed contacts, along with the location and other key information, in less than a second. According to the findings, such a system might be useful as a security instrument in such situations [12].

2.1.4 Preliminary: Blockchain

Blockchain is comprised of a series of ***blocks*** in which each holds some sort of digital information. Such digital information often represents ***transaction-related information*** (e.g., in this case, the transaction will include registering a complaint, verifying a complaint, investigating a complaint, and so on. So, the block will actually store any information involved in such transaction e.g., documents with timestamps, evidence, and so on) and ***information related to the users*** involved in the transaction (e.g., in this case, users may include victim, accused, investigation committee, and so on. The complaint process cannot be completed without the involvement of these users). Therefore, a block stores user information with their public or private key as an identity in the chained network [13].
Blockchain manages a distributed ledger in such a way that each transaction or block is ***uniquely identifiable***, i.e., a hash table is maintained independently to ensure that each transaction complies with some agreed cryptography algorithm. The first block in the blockchain is termed the ***genesis block***, yet it follows certain rules. The hash of the previous block is included in the header of the following block on the blockchain. This aspect of maintaining blockchain ensures that information cannot be edited without altering any information in previous blocks, protecting against attacks. The blockchain ledger also records the timestamps of each transaction, thus altering the block's state indicates a new transaction. If any information is deleted or altered, the chain becomes invalid while the transaction counter is incremented and the entire transaction is completely altered [14].
Unless the transaction or block is validated via ***consensus algorithms***; it couldn't become a part of the blockchain. All transactions in centralized systems are controlled by a central authority. However, blockchain is not decentralized in its nature without using a consensus algorithm for validating transactions or blocks, e.g. Proof-of-Work, Proof-of-Stake, or Proof-of-Authority [15]. Each node inside the network must participate and vote in such an algorithm, which results in an agreement that is favourable to all nodes. In an essence, consensus algorithms are the ***heart of a decentralized ledger***, ensuring that the blockchain system is fully decentralized. The node that validates the blocks is referred to as a ***miner***, and the process of doing so is known as ***mining*** in the blockchain network [16].

Once a block has been verified, the transaction is sent throughout the network, where each transaction is identified by some public key. In the blockchain, users are managed via ***public-private key pairs***. The identifier is used to identify a user, also known as an ***address***; generated using a cryptography hash of the public key. All of a user's transactions, on the other hand, are signed with the user's private key, which is then verified and recorded in blocks before being broadcast to a blockchain network [17].

2.2 Literature Review

Blockchain was firstly used for only peer-to-peer digital fund transfers while enabling the inclusion of auxiliary data for representing the transactions as a digital asset. Initially, there was limited support for programmable transactions in blockchain technology [18]. But over time, different blockchain solutions came to the fore, such as Ethereum [19], enabling the adoption of such technology for challenging solutions using smart contracts [18, 20].

The smart contract is simply a written code or script stored on-chain in a blockchain network; executes when certain predetermined contractual conditions meet. The written contract digitizes and automates the agreements between parties that often do not trust each other [21] . Smart contracts are implemented in a decentralized way without depending on any central authority for enforcing the agreements, thus saving time and resources [22].

Due to the inclusion of these contractual agreements, blockchain now could be used widely for a range of financial goals: including but not limited to trading, lending, borrowing and investing. Different emerging applications of blockchains include enterprise resource planning, human resource management, insurance management, security and privacy, democratic accountability, privacy-aware digital voting systems, identity management, criminal record management system, E-FIR systems, ubiquitous computing, and intelligent systems, to document a few [18, 23, 24, 25, 26, 27].

2.2.1 Combating digital deception using blockchain

A recent study has presented a blockchain-based solution for mitigating evidence spoliation and infringement. The study has uncovered the fact that evidence spoliation ensues in most countries wherein evidence is still paper-based or in physical witness form. Spoliation generally takes three forms: the destruction of evidence, the withholding of evidence, or the tampering or fabrication of evidence. Most of the time, it is problematic for the evidence provider to come out and provide evidence against a high-profile case. In such scenarios, protecting the evidence provider's privacy is more critical. The proposed blockchain-based system empowers citizens and whistle-blowers from the public to come forward and provide evidence anonymously, without fear of repercussions or expo-

sure. It will ensure that only authorized entities have access to the evidence and the provided evidence are tamper-proof [28].

Another research project has presented a blockchain-based trustworthy video surveillance system since the video plays an important role in restoring the truthfulness of any crime or incident. However, the reliability of video evidence is dwindling since most unwelcoming attackers distort original videos and post them on social media to manipulate the public and government authorities. The proposed Video-Chain system provides video credibility while implementing traditional blockchain features. Each video in the chain will have a cryptography hash and only authorized users will be able to decrypt the encrypted video in blockchain i.e., no one will have the right to tamper with or delete the video evidence [29].

A similar study proposed a deep learning-based blockchain network to overcome propaganda, lies and fake news; since deep-fake and fraudulent information sharing on social media is a prevalent concern in such evolving digital world. It is unreliable to depend on any centralized method for detecting false news and media. As a result, this study recommends the adoption of a decentralized system – the hybrid model of deep learning and blockchain system – to ensure the credibility of news. The system introduces three main modules: a reporter, analyzer and validator. The reporter is responsible to report the news and relevant evidence to the system. A deep learning-based analyzer that will ensure the credibility of the news by considering the ranking and wordlist from only authorized sources. And lastly, the validator will be responsible to validate the news based on the analyzer's results and ranking. By keeping only valid and authenticated news on a blockchain, the proposed system ensures the credibility of news and provided evidence. Such a method may help in filtering fake news and can control the spread of fake news, particularly on social media platforms [30]. Moreover, there are various studies that have worked on the same problem of filtering and controlling the spread of fake news on social media using blockchain technology, to cite a few [31, 32, 33].

Recent studies have encouraged the adoption of blockchain in the health and medical insurance sectors. Because of the services provided by policyholders, the influence of health insurers is on the rising trend since the cost of healthcare is at its peak. National Health Care Anti-Fraud Association (NHCAA) has reported that insurance providers incur billions of dollars in financial loss every year. There is no check and balance at the end of insurance providers; clients typically take advantage of this and often provide fake information in order to force them to pay for false claims.

Many research studies have come up with a blockchain-based solution to deal with the problem of rising insurance fraud in recent years; by introducing a decentralized network for storing information from all insurance providers. It facilitates the real-time monitoring and evaluation of consumers' information, as well as providing immutability and privacy to patients' information and records [34, 35, 36].

Keeping in view the adoption of blockchain technology in the above scenarios, the existing literature highly encourages the use of blockchain to combat digital deception. While considering the problem

statement of the current study, the aforementioned literature is motivating the use of blockchain for detecting fake documents or complaints before putting these on the blockchain system when registering harassment complaints.

2.2.2 Human Resource Management using blockchain

The existing literature in human resource management encourages the adoption of blockchain technology for different organizational concerns. Traditional encryption technology, along with blockchain technology, has been used to address the issue of credibility in personnel management.

The paper presents a Blockchain-based human resource information management framework that enables employees to exchange their details with corporations. Job seekers hoax their expertise, previous employment records, academic qualifications, and job descriptions to pique the company's attention. The proposed blockchain-based system helps in the verification of all details, including but not limited to certifications, credentials, references, academic degrees all the relevant documents, thus providing reassurance and an effective traceability mechanism for the organization [37].

Another research has suggested a Global Qualification-Competencies Ledger employing Blockchain framework, which enables the efficient management of a qualification-competence record. An individual's expertise and qualifications are acknowledged in several different certifications. It may include participation certificates for different competitions and contests. Assessing and acknowledging all of an employee's competencies and qualifications is a potential concern for the individuals, and for the authorized stakeholders including employers and government institutions looking for specific competencies. Such a global ledger might be an acceptable and effective solution to the current recruitment challenges i.e., maximizing personnel recruitment, assessing personnel competencies and boosting job opportunities for individuals [38].

Related work has also proposed a blockchain-based recruitment and resource management framework for validating and assessing applicants' profiles based on previous workplaces, contractual agreements, and corresponding organizations. The profiling is done in accordance with the company's recruitment standards, and the system ends up generating a ranked list of verified and skilled professionals for the open positions in an organization. If the system detects any fake data, disruptive behavioral issues, or a criminal history against the applicant, it will automatically discard that profile and continue ranking the other profiles. This blockchain-based recruitment and human resource management system is considered to be a promising solution to help firms in their managerial and personnel recruitment processes [39].

Another study, on the other hand, proposes a blockchain-based approach for handling and monitoring temporary employment contracts, with the goal of ensuring the inclusion of all the participants, respecting the relevant laws throughout the agreement. It will provide employees with justifiable and lawful reimbursement (including taxes) for their quality of work and assistance in case the employer

seems to be bankrupted [40].

Given all of these applications in human resource management, it is evident that a blockchain-based framework may be used to propose an effective harassment complaint system for tracking and registering complaints without the need of an intermediary. The present studies have also suggested that all relevant documents and information should be verified and authenticated before being evaluated or reviewed. Though there is no literature on the subject matter, the related studies encourage the adoption of blockchain systems in situations where transparency, traceability, and autonomy seem to be indispensable.

2.2.3 Blockchain-based Smart Voting and Record Management

A study by Bosri and Uzzal (2019) introduced a blockchain-based voting solution that supports a safe and convenient election while protecting voters' privacy, with seven entities: Election Commission, Voters, Voter Authentication Unit, Voting Unit, Voter Confirmation Unit (polling agents), Vote Result, and Vote Publish Unit [41]. Similarly, Alvi and Syada Tasmia (2020) suggested a Privacy-Aware Digital Voting System based on Blockchain with just six units: registration, voter, voter authentication, voting unit (as a primary component for validating the credibility of votes), vote counting, and publish result unit [42].

Tasnim and Omar (2018) suggested a blockchain-based CRAB protocol that guarantees security and privacy for criminal records and permits only specific entities to access the data. In this protocol, the data sender will be a police station, a court, a law enforcement agency, or the armed forces. The Functional Unit is the primary component that verifies and encrypts data before putting it into the blockchain [43]. The similar kind of work has been proposed in some other studies highly encouraging the use of blockchain for recording criminal records [44, 45, 46]. The proposed system will have the Department of Forensics as a primary unit; to verify the evidence and ensure the credibility of complaints before putting them into the blockchain.

A research work by N. D. Khan and Chrysostomous (2020) proposed a Smart FIR blockchain-based system that guarantees a reliable and efficient way for reporting documents concerning cognizable offences. The principal objective of this suggested model is to avoid fake registrations; and provide authenticity to e-FIR evidence via blockchain, with the following core functionalities: registering police stations, user filing e-FIR, admin approving transaction, and Handling False e-FIR. The relevant work has also been done in a recent work that also employed blockchain technology for storing FIR documents in a decentralized network. The proposed system for the current problem will also avoid fake registration of harassment complaints by allowing this system to track timestamps of submitted files and evidence [44].

2.2.4 Blockchain and its legal Implications

While investigating the interconnection between Computer Sciences and Law, Jat Singh (2020) aims to draw attention to blockchain technology and its legal consequences and presents an overview of how blockchain technology works and should be deployed in various ways to develop solutions. The purpose of this paper is to educate lawyers and other professional advisers about blockchain technology so that they can provide solutions; educate blockchain technology users about conventional legislative challenges and potential implications [47]. This study plays an important role to support the objectives of this study i.e., there should be an effective solution that strictly implements [Act IV of 2010] to prevent harassment at workplaces.

Recent research work has suggested the use of a blockchain system for proposing a tax management framework for Pakistan to provide accountable and efficient tracking and auditing of payable taxes. This decentralized system considering the legal implications of Pakistani law allows all the authorized parties including banks, government entities, institutes and relevant companies to access and logging the relevant details regarding individual's payable taxes. It helps in controlling fraud cases that mostly happen in senior management; making sure that no tax record is editable for any taxpayer. If any illegitimate user attempts to modify or edit the record with the ulterior intent; the court should be notified, and a case may be made against the individual under Pakistani law [48].

Chapter 3

Methodology

In this chapter, a detailed overview of the research methodology, the overview of the system and the proposed framework has been presented

3.1 Research methodology

This research study will follow the following research methodology to achieve the mentioned objectives of this research work (See Figure 3.1)

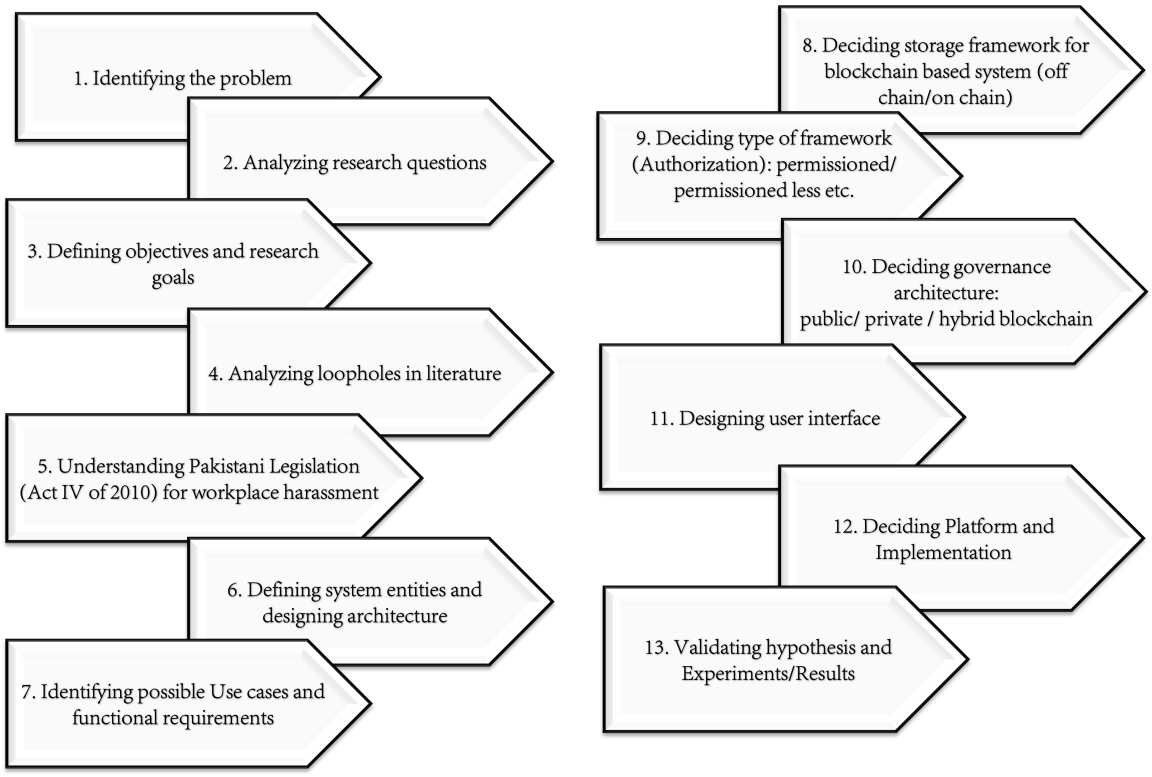

Figure 3.1: Research methodology for current study

3.2 System Overview

In the current situation, victims have to file a complaint against the harasser by reporting all concerns of sexual harassment or inappropriate sexual conduct to the HR director or a supervisor/manager of the organization. The higher authorities in such situations tend to resolve the issue informally, and

such a trend is normalizing the harassment as the accused is not given the punishment according to the law. According to different case studies, the current procedure for registering and enquiring harassment complaints at workplaces is not effective enough to ensure justice as per the law. To the best of our knowledge, there is no such system that strictly implements PAHWAWA 2010. Considering this fact, there is a dire need for an alternative decentralized system that should empower the victims to file such complaints without fear of being withdrawn by any higher authority. The unique perspective of the proposed system includes anonymity, confidentiality, and privacy for the victims' information (while considering the dignity and reputation of females in society); thus, choosing a blockchain-based system seemed to be an effective alternative in such a scenario, with the following unique perspective as per legislated law:

- **Data privacy:** The system should ensure data privacy while adhering to the Act (PAHWAWA 2010), which mandates that "all the statements/complaints and evidence acquired in the inquiry process shall be considered confidential." All the documented and recorded information from the complaint process should not be exposed to unauthorized entities, including the name of the victim (while considering the woman's modesty and reputation in the first place).

- **Decentralized and tamper-resistant system:** The system should be decentralized in order to empower victims, i.e., there should be no control of the employer or higher authorities who can withdraw complaints without the complainant's authorization. The blockchain system will ensure the immutability of evidence, i.e., once it is generated, it should not be modified or tempered. All the pieces of evidence should be stored with a timestamp to maintain the credibility of the evidence.

- **Data accountability:** The system should make certain that no stakeholder has complete control over the data. Instead, each stakeholder will just hold a copy of the complaint information while considering the fact that no one should be allowed to misuse any information.

- **Evidence Verification:** To avoid registering fake complaints, the system should provide an evidence verification mechanism or the inclusion of third-party law enforcement agencies in the complaint system to ensure the credibility of registered complaints. The system should ensure that no fabricated documents or evidence are provided by any party to support the case; if this occurs, the person should be punished in compliance with the law.

3.3 System Design

The objective of this study is to propose a harassment complaint system that takes into account all of the users specified in Act IV and strictly follows and implements Pakistani legislation [Act No. IV of 2010 - Protection against Harassment of women at the Workplace Act, 2010] enacted specifically for

this concern. The investigation procedure as legislated by GoP according to Pakistani Act IV of 2010 has been presented in detail (See Figure 1.1).

The system is supposed to consider the complaints only if the victim has any supporting evidence while considering the fact that if a victim is experiencing harassment at work, there is a possibility that the victim may record or capture any evidence (or any colleague can assist in this case). But on the other hand, a new entity (Department of Forensics) has been introduced to this system to ensure the credibility of provided evidence. The notion of this modification is to verify all digital documents to ensure that the pieces of evidence are not fabricated, hence avoiding the registration of fake harassment complaints.

The proposed **Blockchain-based Harassment Complaint System** will allow the victim and all the stakeholders to keep the record of the submitted complaint until it is resolved. The system will make sure that accused has been given the appropriate punishment thus preventing such cases to happen again in future. It will also empower the victims to register harassment complaints without fear of being withdrawn. In case, if the inquiry committee tends to support the company's reputation or accused profile through any means; the system will allow the victim to take the case to the ombudsman for legal actions against the company. This system could be a promising solution to mitigate such cases and help other states to implement such solutions according to their respective laws.

The current study has proposed *workflow diagram* as per the requirements of PAHWAWA 2010 i.e., it explains the flow of different operations to be performed using the concerned system (See Figure 3.2).

There are **six** main entities in this system according to *Act IV of 2010*: ***Complainant, Department of Computer Forensics*** *(for Evidence Verification)*, ***inquiry committee, accused, competent authority*** and ***law authority***.

1. **Complainant:** The victim will file the harassment complaint along with evidence with valid timestamp (Evidence could be in any form i.e., CCTV footage, voice or video recording during the misconduct or medical report in case of physical abuse). After receiving the final decision from the inquiry committee and competent authority, the only victim will have the right to close the case; the victim can open the case again to pursue legal action (opting for ombudsman to pursue the case) if he or she is dissatisfied with the investigation results.

2. **Department of Forensics:** The system will make sure that no fabricated evidence is provided by both the parties to support the case. This entity will help in ensuring that the no complaint with mala fide intentions is registered. The system will verify the creditably of complaint, all the documents and evidence shared by each party before handing over the documents to the Inquiry Committee. If there will be any fabricated evidence, then the system will hand over the case to ombudsman for declaring the punishment according to the law.

3. **Inquiry Committee:** The system will pick a subset of higher authorities (outside the de-

partment or organization); consisting of three members (at least one female) according to the Pakistani Act 2010. This committee will be given the charge to communicate charges and allegations to the perpetrator*within seven days*, investigate the case after receiving required documents and evidence from both the parties and generate a formal written report of the case to be shared with the competent authority to impose the recommended penalty (if the charges are valid).

4. **Perpetrator:** The perpetrator will be allowed to submit the written defense against the charges and allegations within seven days; along with evidence. The system will cross-verify the evidence and written defense before proceeding further.

5. **Competent Authority:** There will be a competent authority that would be responsible to impose the penalty recommended by the inquiry committee.The system will allow the authority to track all the complaint documents, evidence, and findings of Inquiry Committee; allowing the authority to communicate the course of action/ penalty to all the stakeholders.

6. **Ombudsman/ Law authority:** There will be a law authority to pursue legal actions in case if victim is not satisfied from the organization's decision. The system will allow the victim to share the formal written report/Committee remarks along with all pieces of evidence to the legislative body for further proceedings and/or in order to declare the legal punishment for the accused.

This proposed decentralized and tamper-resistant system would enable victims to register a harassment complaint, which will be investigated while strictly following and implementing Pakistani legislation (Act IV of 2010). It would not only reduce the organization's efforts in manually monitoring and investigating such complaints but will also make it much easier for victims to register such complaints using this system instead of going to legislative authorities to seek justice.

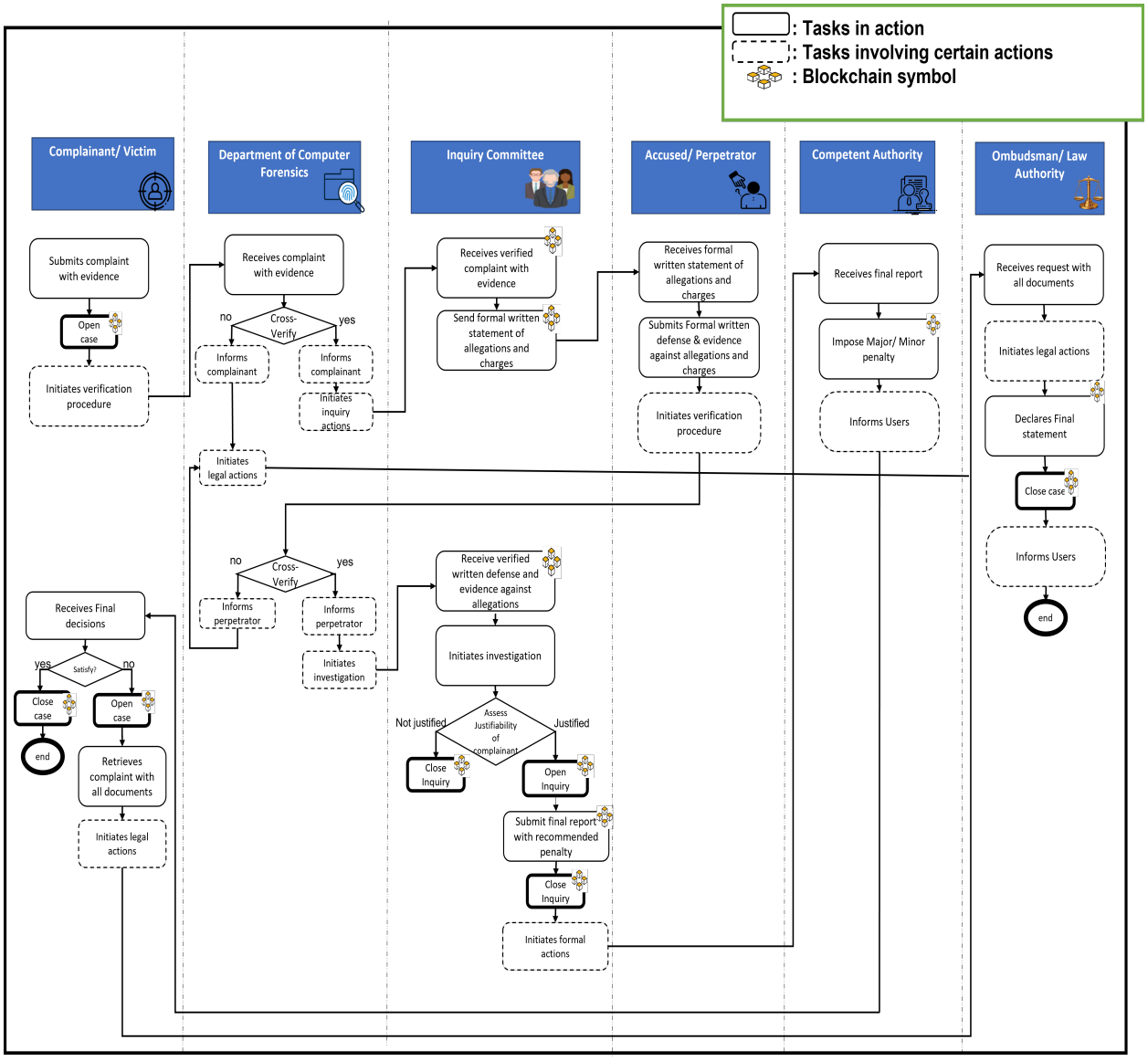

Figure 3.2: Proposed blockchain-based Harassment Complaint File System

Chapter 4
Experimental Results

This chapter is divided into two parts. The first section will introduce the scope and basic functional requirements of the proposed proof of concept. The second section will highlight the specification and details of the technologies and tools used for implementation purpose; and the smart contract (written so far) with all the required details.

4.1 Proof of Concept (PoC)

The Proof of Concept plays a huge role in the Blockchain community since adopting a blockchain-based solution involves mass production, which may include money, time, and a lot of computing resources. At first impression, blockchain technology seems to be fascinating to every developer while exploring a decentralized solution. However, there are several other limitations and constraints that question the effectiveness and productivity of the proposed solution in a real setting or environment.

As a result, before deploying the proposed solution in a real environment, researchers and professionals tend to evaluate the proposed Proof of Concept on previously designed public blockchain platforms or standards. If the solution provides effective results in such platforms, it's indeed feasible to invest in additional resources for real-world implementation.

The current study has also proposed a Proof of Concept that is exactly tailored according to the legislated law [Act IV of 2010] [2]; for testing the feasibility of the proposed solution.

The steps involved in prototyping a Proof of Concept include:

- **Identify Requirements:** The first stage is to determine the proposed solution's functional and non-functional requirements. The key features expected from the blockchain system are identified by defining the requirements. The ***functional requirements*** for the proposed PoC have been presented in detail in the next sections. Once feature requirements are defined, the next step is to choose the blockchain protocol.

- **Select a blockchain protocol:** There are the blockchain solutions that are currently available in the market and comply with the integral protocols, including security, network, and consensus protocols. Using such protocols limits the additional cost, time, and computational resources to a minimum while ensuring that the proposed system will work in a real-world setting or not. Among top blockchain solutions e.g., HyerLedger, R3 Corda, Ethereum, Ripple etc, this study is enabling the use of the ***Ethereum framework*** [19] for prototyping the PoC and verifying the feasibility of the proposed solution. It is a public blockchain technology enabling the use of

Proof-of-Work as a consensus algorithm within the blockchain.

- **Define the Governance Architecture:** The next stage is to choose the blockchain architecture that will be employed in the proposed system. It is not worth pointing the use of private or hybrid blockchain technology for this challenge based on the problem description of this study. The proposed system emphasizes the hypothesis of managing complaints without a central authority. In both private and hybrid blockchains, an administrative entity manages the network in some way. The present study will promote the use of ***public blockchain*** for the registration of harassment complaints. The current study, however, suggests using off-chain storage to preserve the confidentiality and anonymity of registered complaints without compromising efficiency. The sensitive data will be stored off-chain while the hashes of documents will be stored on-chain; considering the work from Gervais [49]. The highlighted work implied the use of a secure cryptography algorithm to generate the hashes. On the other hand, the use of a hash function will also incentivize each document to have a unique message digest or hash value, even if the content is somewhat altered. It will contribute to ensuring that evidence is tamper-proof and help in maintaining the integrity of documents stored off-chain.

4.1.1 Scope of proposed PoC

This section introduces the scope and functional requirement of the proposed system i.e., *"Harassment Complaint System in accordance with Pakistan Legislation ACT IV of 2010"*. The Legislation *[Act No. IV of 2010 - Protection against Harassment of women at the Workplace Act, 2010]* enacted in 2010 has been explained briefly in Chapter 2. Considering all the major findings and guidelines under this law [2], this section will introduce the functional requirements for the proposed system.This PoC will ensure that all actors participating in the proposed system have access to all of their legal rights.

4.1.2 Functional Requirements of PoC

The PoC discussed here is tailored to the cited legislation of Pakistan [2]. However, the Functional Requirements along with the description have been provided below against each finding from the law.

1. *Each organization shall constitute an Inquiry Committee within thirty days of the enactment of this Act to enquire into complaints under this Act.*

2. *In case a complaint is made against one of the members of the Inquiry Committee that member should be replaced by another for that particular case. Such member may be from within or outside the organization.*

3. *In case where no competent authority is designated the organization shall within thirty days of the enactment of this Act designate a competent authority*

4. ***Procedure for holding inquiry-***

   (a) *The Inquiry Committee, within three days of receipt of a written complaint, shall–*

   - *communicate to the accused the charges and statement of allegations leveled against him, the formal written receipt of which will be given;*
   - *require the accused within seven days from the day the charge is communicated to him to submit a written defense and on his failure to do so without reasonable cause, the Committee shall proceed ex-parte; and*
   - *enquire into the charge and may examine such oral or documentary evidence in support of the charge or in defense of the accused as the Committee may consider necessary and each party shall be entitled to cross-examine the witnesses against him.*

   (b) *The following provisions inter alia shall be followed by the Committee in relation to inquiry:*

   - *The statements and other evidence acquired in the inquiry process s*
   - *The Inquiry Committee shall give its findings in writing by recording reasons thereof.*

Considering above findings from Law, each organization is responsible to designate an Inquiry Committee and Competent Authority for the purpose of investigating the cases registered under harassment complaints. i.e., Inquiry Committee should consist of three members including one female member, a senior representative of employee and a member from senior management [2].
The Functional Requirements against above findings has been summarized below in two scenarios. PoC part (i) in Table 4.1 describes all the functional requirements required for filing the complaint and fulfilling all the necessary requirements before initiating the investigation process. However, Table 4.2 highlights the functional requirements in Investigation Process till the end of the complaint process.

4.2 Interface Design and Smart Contract

The initial interface design of the system has been presented in this section with all the tentative test cases in order to strengthen the notion of implementing such a system. The main login page for all the concerned users has been shown in Figure 4.1.
The interpretation of the complainant profile has been shown in Figure 4.2; in which the victim is required to submit the complaint along with evidence. However, the evidence is considered to be

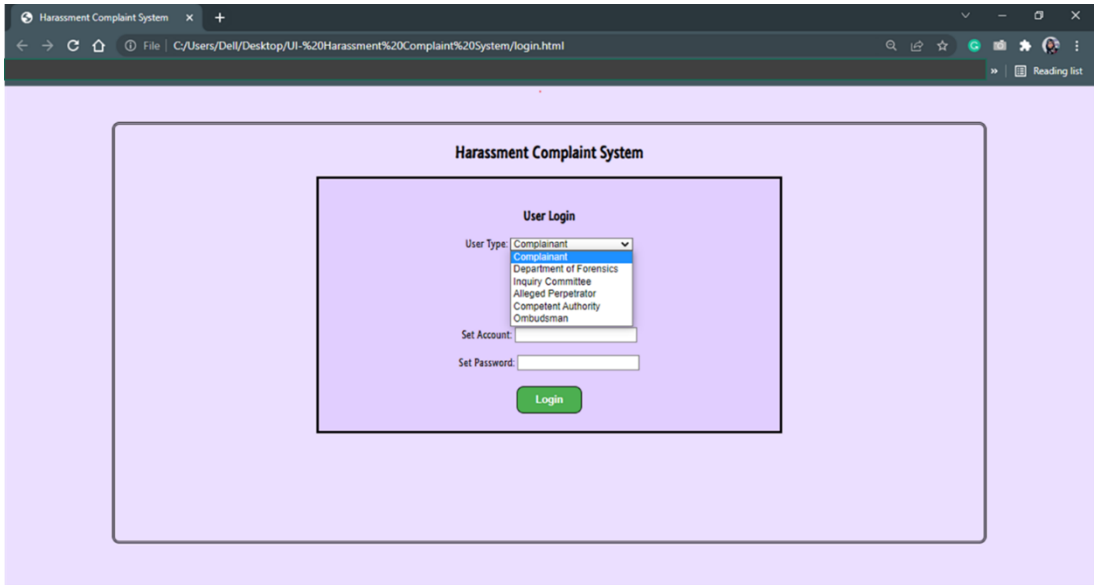

Figure 4.1: Users' Login Page

mandatory in this case because of the fact that we are proposing a system for a workplace and any victim being a part of the same workplace harassed by any colleague or a higher authority repeatedly; can easily record any such harassment communication or gesture using some camera or microphone (and/or any close friend or colleague may assist the victim in this case). Moreover, after submitting the complaint, the victim can track the complaint status to be enquired as per the legislation (presented briefly in Figure 1.1).

The different use cases have been shown in Figure 4.3), in which the complaint status will be 'Opened' only if the Department of Forensics will cross-verify the complaint and evidence (and also ensure that evidence has not been tampered). Once the status will be opened, the copy of the complaint and evidence will be shared with the inquiry Committee to further enquire about the credibility of the complaint. However, only the complainant is allowed to close the complaint status as 'Closed'. Otherwise, if the victim is not satisfied with the decision of the Inquiry Committee, she can pursue legal actions and can 'Request Ombudsman' while sharing all the details and authority's decision with the legislative body (See Figure 4.3)). After the final decision of the Ombudsman, the complaint status will be set as 'Closed' automatically.

The tentative interface design for the Department of Forensics i.e., for verifying all the documents and evidence has been shown in Figure 4.4). When the Department of Forensics will verify the complaints, it means that provided evidence is not fake and the system will share the verified document along with evidence with the Inquiry Committee for further investigation. On the other hand, if any evidence is found to be fabricated then these cases will be sent to the Ombudsman for deciding the punishment against such mala fide attention (as legislated under the same Act).

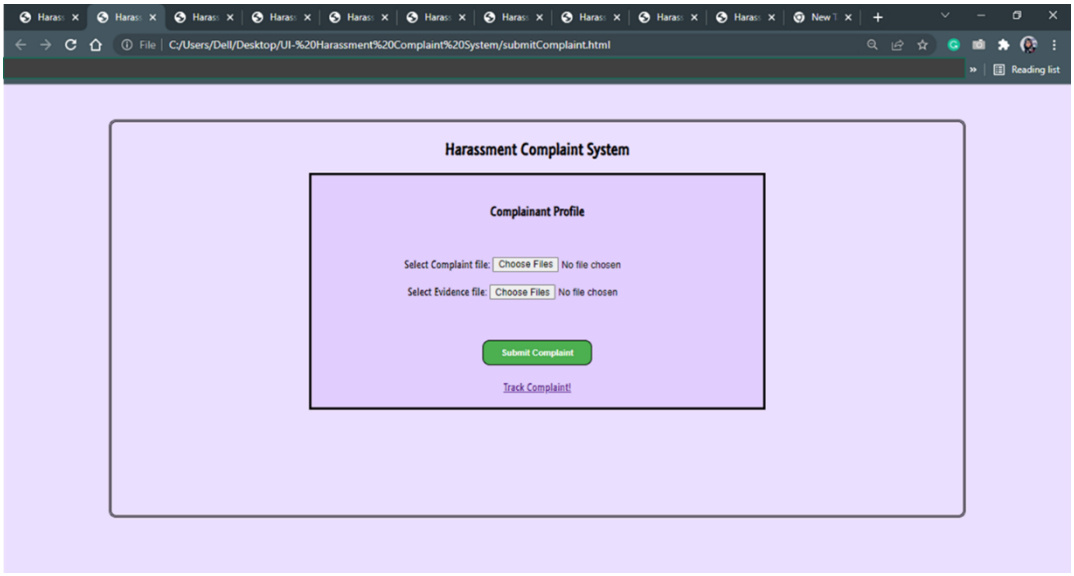

Figure 4.2: Complainant's Profile

The tentative interface for Inquiry Committee has been presented in Figure 4.5. The Inquiry Committee is legislated to inform the perpetrator and send notice of the charge and allegations against him (See Figure 4.6). On the other hand, upon receiving the notice from Committee, the perpetrator can see all the complaints filed against him and track the status of the complaint (See Figure 4.7). However, In Figure 4.8, the perpetrator is legislated to submit the defense document (along with evidence) against the allegations made against him (within seven days). Once the perpetrator will submit the defense with evidence and is verified by the Department of Forensics; all the documents will be shared with the Inquiry Committee for further investigation. The different use cases have been shown in the following Figure 4.5, wherein once the Inquiry Committee make the final report of the case findings; it will be allowed to share it with the Competent Authority to impose the suggested penalties. The Inquiry Committee will be allowed to update the status of the Inquiry as 'Closed' to ensure that case has been investigated thoroughly and the complainant has to wait for the Course of action from the Competent Authority). The tentative interface design for the Competent Authority and Ombudsman to enquire about the complaints has been shown in Figures 4.9 and 4.10 respectively.

For implementation purposes, the current study has used **Remix** platform to implement and deploy the smart contract relevant to the above functionalities. The smart contract is written using the latest version of **Solidity** language i.e., *version 0.8.12*; which is a fully developed version. It is implemented to store all the main documents to be used in this process. However, the documents will be stored offline; given that all the hashes of the verified documents will be stored on-chain in variables of type ***bytes32*** (See Figure 4.11- lines 21 to 28).

Moreover, the addresses of six entities as per the law are also recorded in variables of type ***address*** (See Figure 4.11- lines 14 to 19). The addresses are the public keys of the Ethereum accounts to be

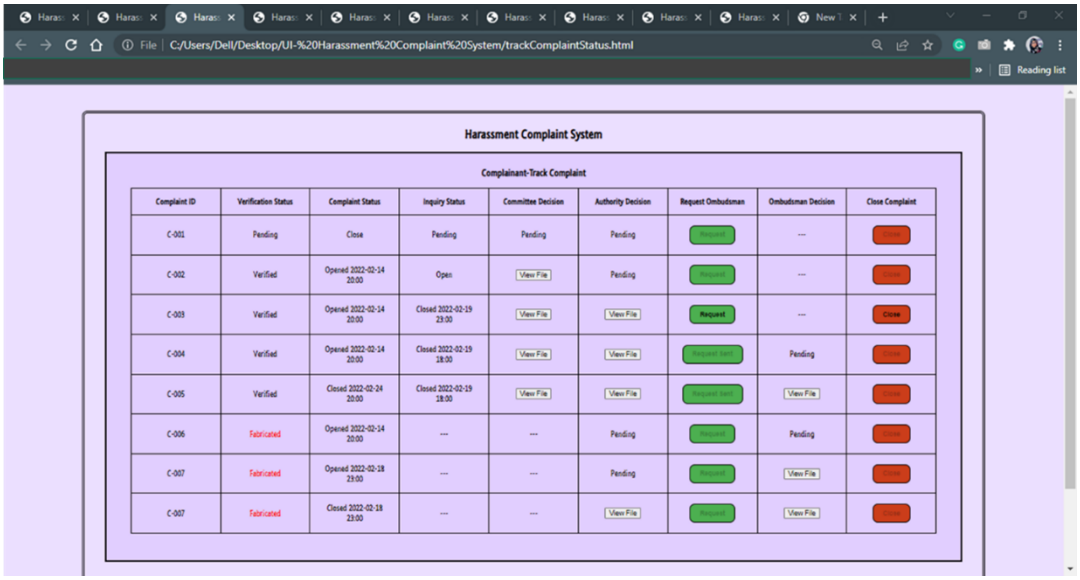

Figure 4.3: Complainant- Track Complainant

used by different stakeholders. When a user interacts with the system, the smart contract validates the account's address to determine whether or not the user is permitted for the specific transaction.
Lastly, the time and date for each transaction are also recorded in a variable of type ***uint*** (See Figure 4.11- lines 4 to 12). Since the enacted law restricts the completion of an investigative process for a particular time-frame, this feature of time-stamping each transaction will help the system in tracking the status of the filed complaints.
In most transactions, more than one users are accountable for the completion of a transaction. For such transactions, the ***mapping*** of *address* and time to date variables represented in *uint* is recorded (See Figure 4.12- lines 30 to 38).
When a complainant makes a complaint using this system, the *constructor* of the smart contract is triggered. The complainant's address, as well as the time and date of filing the complaint, is recorded. The **constructor** as shown in Figure 4.13 (line 40-43):

- Sets the *complainant* address as the user that is initiating the transaction. The address of the complainant is referred to the value *msg.sender* (line 41).
- Saves the *timeAndDate* of initiating the complaint process in the dateTimeCreated variable; setting the *timeAndDate* to be the current time (line 42).
- Saves the hash of the complaint document in *complaintDocHash* variable as provided by constructor argument - attached by the complainant (line 43).

The smart contract written so far is briefly described in the section. However, the application interface will be designed later using **Electron** platform [50] (that allows cross-platform web development) for

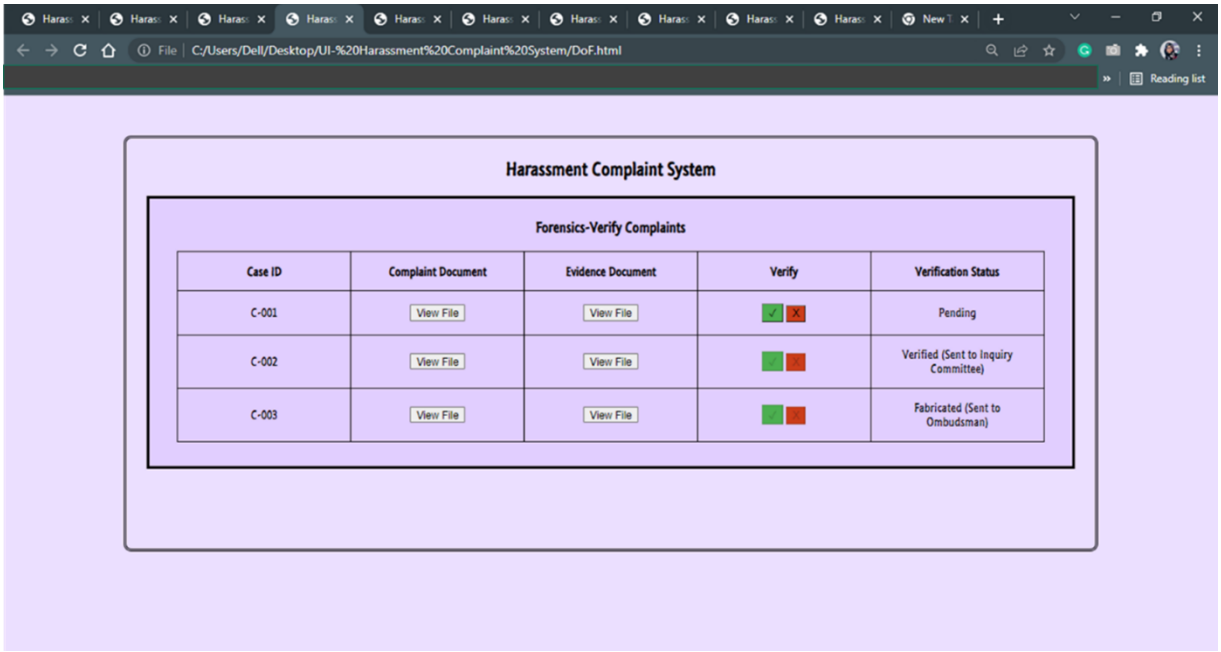

Figure 4.4: Department of forensics- verify and share verified / fabricated evidence

testing the functionality of the smart contract. As the system is still under implementation; cost analysis, gas consumption, and vulnerability analysis of smart contracts will be performed later for the performance testing of the proposed system.

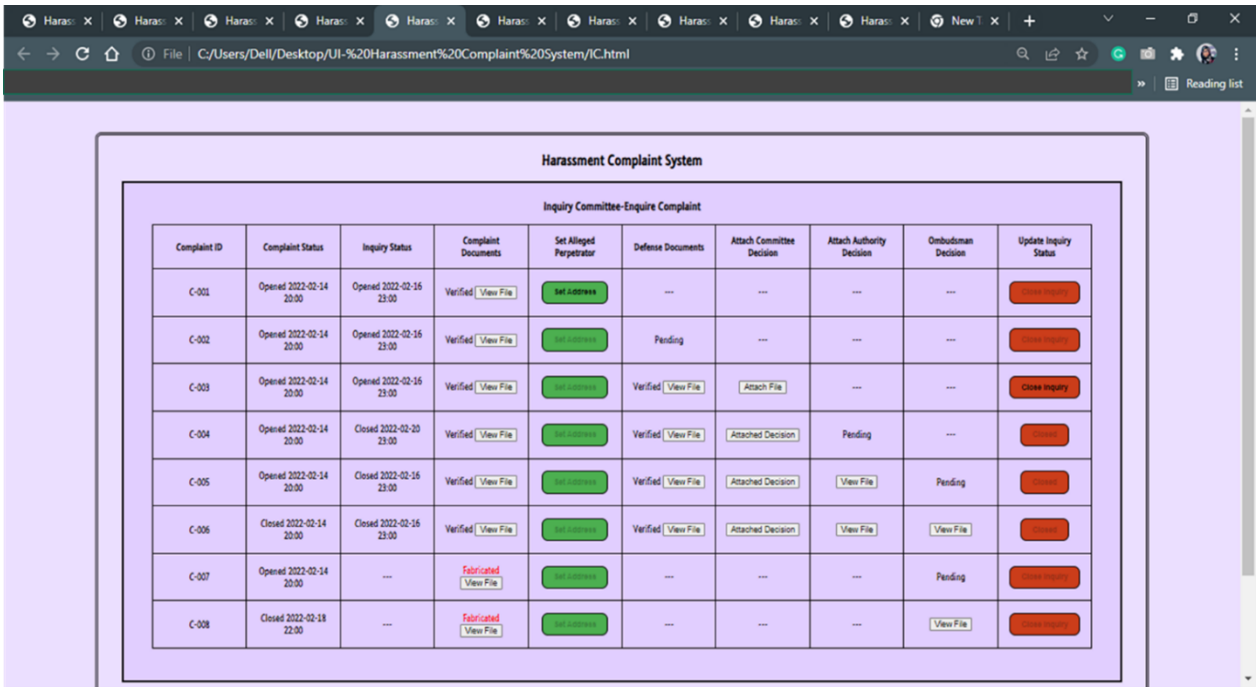

Figure 4.5: Inquiry Committee- Enquire about complaints

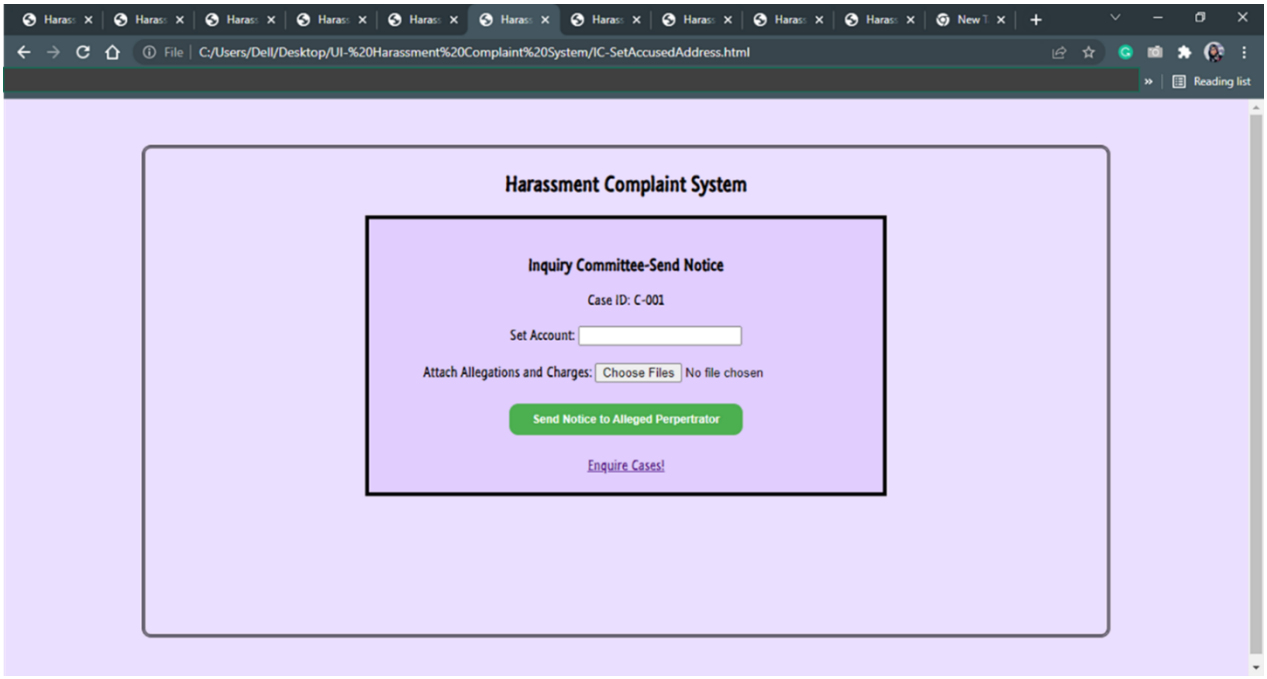

Figure 4.6: Inquiry Committee- Send notice to perpetrator

Table 4.1: Functional Requirements for proposed PoC (part i)-Filing Complaint

FR	Description
FR-1	*The system should enable the feature of setting the addresses of actors for designating them as an Inquiry Committee and a Competent Authority.*
FR-2	*The system should allow to update the addresses of Inquiry Committee members in case if the complaint is against any of the member of the Inquiry Committee member.*
FR-3	*The system should allow the complainant to file the complaint along with possible pieces of evidence.*
FR-4	*The system should record the time and date of initiating the complaint.*
FR-5	*The system should send the copy of complaint and evidence to Department of Computer Forensics for cross verification.*
FR-6	*If verified, the system should update the status of complaint as open, record the date and time, and should store the generated hashes of documents in the system.*
FR-7	*Upon receiving the complaint, Inquiry Committee should share a written notice to alleged perpetrator within next three days.*
FR-8	*The system should notify the alleged perpetrator to submit the defense in written charges within next seven days.*
FR-9	*Upon receiving the defense and evidence, the system should send the copy of complaint and evidence to Department of Computer Forensics for cross verification.*
FR-10	*If verified, the system should update the status of Investigation as open, record the date and time, and should store the generated hashes of documents in the system.*

Table 4.2: Functional Requirements for proposed PoC (part ii)-Investigation and Final Decision

FR	Description
FR-11	*The system should share all the verified documents to the Committee and notify the Inquiry Committee to enquire into the case.*
FR-12	*The system should restrict the Inquiry Committee to submit its finding within thirty days of initiation of inquiry.*
FR-13	*Upon submitting the inquiry report, the system should update the status of Investigation as close and record the date and time.*
FR-14	*The system should share the copy of findings to Competent Authority and allow it to declare the course of Action to be shared with all the involved parties*
FR-15	*The system should allow both the victim and alleged perpetrator to share their feedback on the decision.*
FR-16	*If decision of victim is not satisfactory, the system should allow the complainant to pursue the investigation using Ombudsman.*
FR-17	*The system should allow the victim to share all the details of case proceeded so far to the Ombudsman and shall update the status of complaint accordingly.*
FR-18	*The system should restrict the Ombudsman to record the final decision and share it with the authorized parties.*
FR-19	*The system should update the status of complaint as close, if the victim feedback from the victim is satisfactory.*

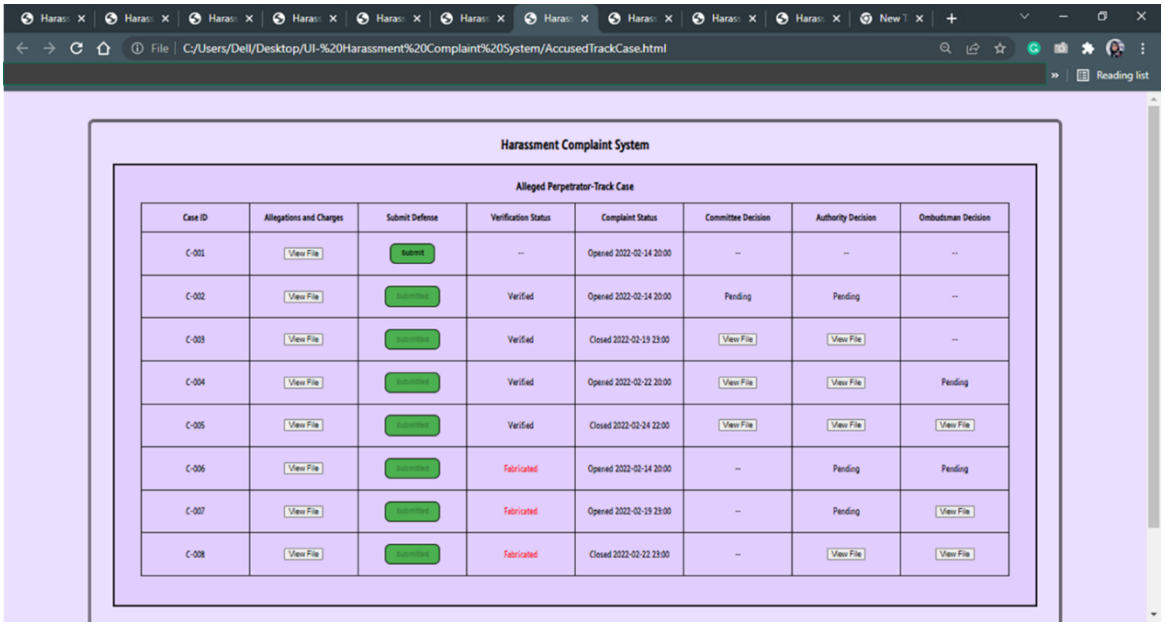

Figure 4.7: Alleged Perpetrator- Track cases

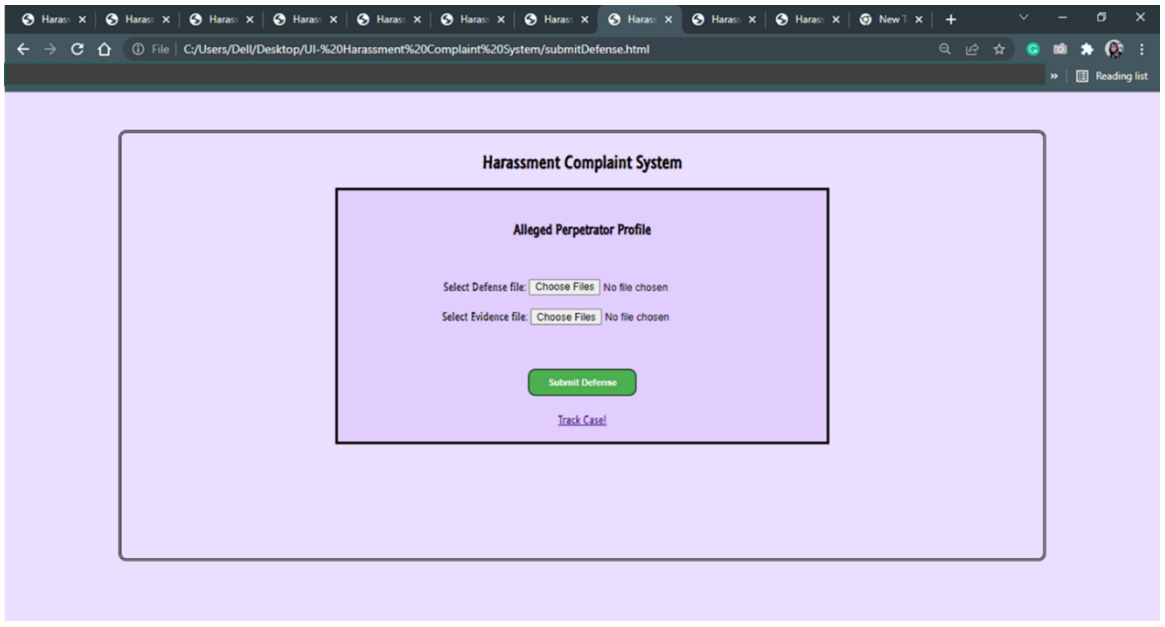

Figure 4.8: Alleged Perpetrator- Submit defense

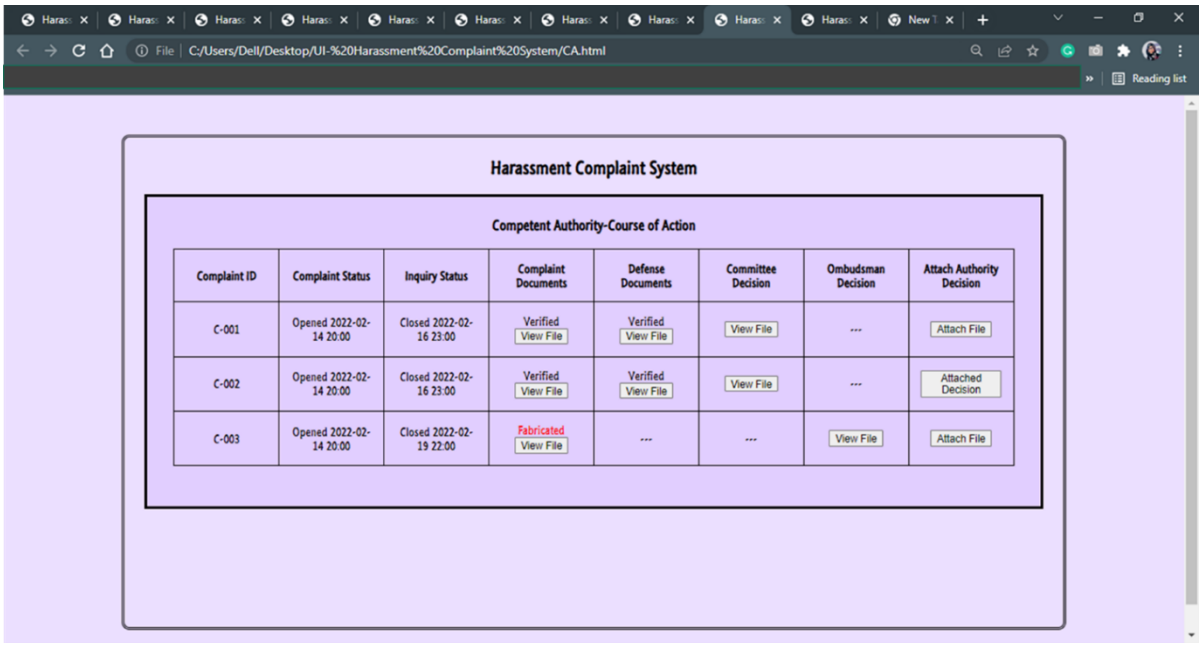

Figure 4.9: Competent Authority- Course of Action

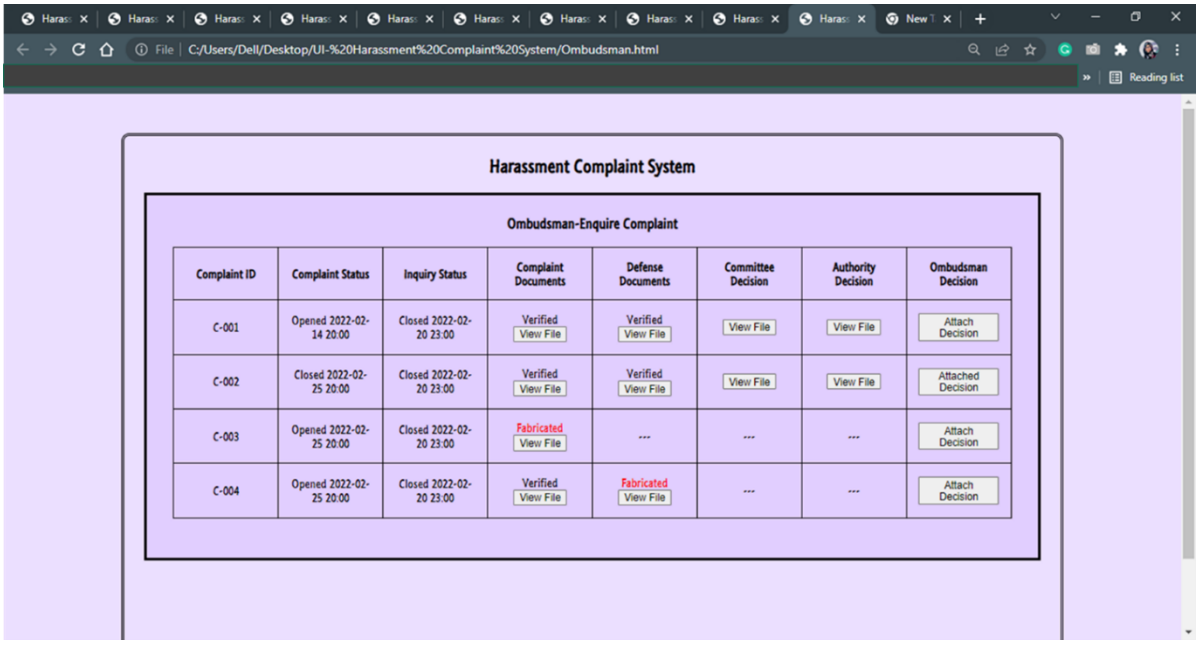

Figure 4.10: Ombudsman- Enquire about complaints

```
pragma solidity ^0.8.12

contract ComplaintSystem{
    uint dateTimeCreated;
    uint timeVerifiedDocFromForensicsComplainant;
    uint timeVerifiedDocFromForensicsPerpetrator;
    uint timeNotificationForPerpetratorDoc;
    uint timeDefenseDocFromAllegedPerpetrator;
    uint timeInvestigationReport;
    uint timeCourseOfActionFromCompetentAuthority;
    uint timeOrdersFromOmbudsman;
    uint timeFeedbackFromVictim;

    address complainant;
    address InquiryCommittee;
    address allegedPerpetrator;
    address CompetentAuthority;
    address LawAuthority;
    address DepofForensics;

    bytes32 complaintDocHash;
    bytes32 VerifiedFromForensicsComplainantDocHash;
    bytes32 VerifiedFromForensicsPerpetratorDocHash;
    bytes32 NotificationForPerpetratorDocHash;
    bytes32 DefenseFromAllegedPerpetratorDocHash;
    bytes32 InvestigationReportDocHash;
    bytes32 CourseOfActionDocHash;
    bytes32 OrderFromOmbudsmanDocHash;
```

Figure 4.11: Smart Contract: Initial variables

```
    mapping (address => uint) userToFileComplaint;
    mapping (address => uint) userToVerifyDocFromComplainant;
    mapping (address => uint) userToVerifyDocFromPerpetrator;
    mapping (address => uint) userToNotifyAllegedPerpetraator
    mapping (address => uint) userToSubmitDefenseDoc;
    mapping (address => uint) userToSubmitInvestigationReport;
    mapping (address => uint) userToIntroduceCourseOfAction;
    mapping (address => uint) userToIssueLegalOrders;
    mapping (address => uint) userToGiveFeedbackOnFinalDecision;
```

Figure 4.12: Smart Contract: Mapping addresses

```
    constructor(bytes32 DocHash) public {
        complainant = msg.sender;
        dateTimeCreated= now;
        complaintDocHash = DocHash;
    }
```

Figure 4.13: Smart Contract: Constructor Function

Chapter 5
Conclusion and Recommendations

This chapter concludes the current research work proposed so far i.e., Introducing the research area, highlighting the problem statement, presenting a detailed related work and literature review along with the proposed solution for the stated problem. This chapter ends with the recommendations of this research work to be considered as future directions.

5.1 Conclusion

Workplace harassment is perceived as a pervasive problem, with devastating psychological consequences that end up creating a hostile environment for victims, negatively impacting employee productivity and well-being. Many companies still have a knee-jerk reaction to harassment claims because they consider it a waste of time and effort that might ultimately damage the company's reputation in front of the public. Even though the Government of Pakistan has introduced a law to promote citizens' rights to respect and decency *[Act No. IV of 2010]*[2]. Since more than a decade has been passed, workplace harassment is still on a dramatic increase. Organizations are unable to effectively enforce the law and fail to offer a sufficiently safe and secure environment for female employees.
Because Pakistan is a patriarchal country, female victims in Pakistan find it difficult to speak out against what has occurred to them because it undermines their dignity and respect in society. If any of the victims file a complaint, they rarely get a satisfactory response from higher authorities, which gradually normalises harassment and forces the victims to switch jobs.
Despite the considerable prevalence of workplace harassment in Pakistan, the current study has explored the Consequences and Antecedents of workplace harassment in Chapter Two. The research has also looked into the different complaint procedures being used to file such complaints. It has included the legally enforced procedure for registering harassment complaints in Pakistan. Moreover, in related work, the recent state-of-the-art solutions for preventing workplace harassment have been considered (See Chapter Two).
Considering the devastating consequences of workplace harassment, the present study's literature review has explored several applications that use a blockchain-based decentralised system to address such problems. As the suggested method focuses not only on filing harassment complaints while respecting the dignity of female employees within society, but it also focuses on the need that no fake complaints be submitted to damage the company's reputation. Given this concern, the study looked at several blockchain applications to avoid digital deception. Furthermore, the relationship between blockchain and law as provided in the literature has been investigated to support the objectives of this research (see Chapter 2).

Motivated by an analysis of relevant literature and the serious consequences of workplace harassment, the present study proposes a Harassment Complaint System that strictly follows the legislation [Act No. IV of 2010 - Protection against Harassment of Women at Workplace Act, 2010] (See Chapter 3). The proposed system is a decentralized blockchain-based system that allows sexually harassed victims to record the process until the complaint is resolved without fear of being withdrawn by the central authorities or employer. Given the privacy and morality concerns of female employees in a patriarchal culture, this system would not allow any unauthorised individual to access any information of victim provided to file a complaint. This system will not only guarantee the dignity of female employees but also ensure that justice will be served in accordance with applicable law.
The Proof of Concept tailored for this system complies with the legislation, which allows victims to continue demanding justice until they are satisfied with the decision of a company's Inquiry Committee. It will ensure that the alleged perpetrator has received the appropriate punishment; if not, the victim will be able to seek justice through the legal authorities (Ombudsman) using this system.The functional requirements of this PoC has been discussed briefly in Chapter 4.

5.2 Recommendations

The focus of this research is to encourage the adoption of a blockchain-based decentralized framework for controlling and preventing workplace harassment. The main objective is to limit workplace harassment while concentrating on the fact that there should not be any central entity to register such complaints. The smart contracts used for this purpose will be able to maintain track of all transactions from authorized parties, time-stamping them and ensuring that no one has the authority to tamper with or withdraw any document or information.
However, the smart contracts have been implemented and deployed on the Remix platform, which is based on the Ethereum blockchain technology. Testing and deploying the system in a practical setting is currently difficult due to limited computing resources. To address this shortcoming, the current work strongly recommends the implementation of the proposed system in a real-world context to evaluate its performance.

References

[1] G. Vijayasiri, "Reporting sexual harassment: The importance organizational culture and trust," *Gender Issues*, vol. 25, no. 1, pp. 43–61, 2008. [Online]. Available: https://doi.org/10.1007/s12147-008-9049-5

[2] Legislation, "The protection against harassment of women at the workplace act 2010," in *PART 1 Acts, Ordinance, President's Orders and Regulations. Legis.Act No. IV*, 2010, pp. 1–10.

[3] M. R. Rokonuzzaman, "Workplace harassment and productivity:a comprehensive role of strategic leadership," *Journal of General Education*, vol. 1, pp. 41–49, 2011.

[4] S. M. Malik and Y. N. Farooqi, "General and sexual harassment as predictors of posttraumatic stress symptoms among female health professionals," 2014.

[5] S. J. Nighat Yasmin, "Workplace harassment: Psychological effects and coping strategies in public and private organizations of lahore-pakistan." *FWU Journal of Social Sciences*, vol. 11, pp. 310–321, 2017.

[6] N. Yasmin, "A study on reporting of sexual harassment by working women in lahore-pakistan," *FWU Journal of Social Sciences*, vol. 12, no. 2, pp. 24–34, 2018.

[7] M. M. Sadruddin, "Sexual harassment at workplace in pakistan - issues and remedies about the global issue at managerial sector," 2013.

[8] Feldman-Summers, "Analyzing anti-harassment policies and complaint procedures: Do they encourage victims to come forward?" *The Labor Lawyer*, vol. 16, no. 2, pp. 307–317, 2000.

[9] A. J. Manuel Velázquez, "The role of work environment authorities in the dynamics of workplace bullying, emotional abuse and harassment," *Pathways of Job-related Negative Behaviour. Handbooks of Workplace Bullying, Emotional Abuse and Harassment*, vol. 2, pp. 1–29, 2018. [Online]. Available: https://doi.org/10.1007/978-981-10-6173-8_19-1

[10] H. J. Do, S. H. Yang, B.-G. Choi, W. T. Fu, and B. P. Bailey, "Do you have time for a quick chat? designing a conversational interface for sexual harassment prevention training," in *26th International Conference on Intelligent User Interfaces*, 2021, pp. 542–552.

[11] S. Sadeh-Sharvit, J. Giron, S. Fridman, M. Hanrieder, S. Goldstein, D. Friedman, and S. Brokman, "Virtual reality in sexual harassment prevention: Proof-of-concept study," in *Proceedings of the 21st ACM International Conference on Intelligent Virtual Agents*, 2021, pp. 87–89.

[12] N. Ahmed, S. A. U. Rahman, R. J. Rony, T. Mushfique, and V. Mehta, "Protibadinext: Sensor support to handle sexual harassment," in *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct*, 2016, pp. 918–921.

[13] A. Haque and M. Rahman, "Blockchain technology: Methodology, application and security issues," *arXiv preprint arXiv:2012.13366*, 2020.

[14] T. Jin, X. Zhang, Y. Liu, and K. Lei, "Blockndn: A bitcoin blockchain decentralized system over named data networking," in *2017 Ninth international conference on ubiquitous and future networks (ICUFN)*. IEEE, 2017, pp. 75–80.

[15] S. Wan, M. Li, G. Liu, and C. Wang, "Recent advances in consensus protocols for blockchain: a survey," *Wireless networks*, vol. 26, no. 8, pp. 5579–5593, 2020.

[16] M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and A. Colman, "Blockchain consensus algorithms: A survey," *arXiv preprint arXiv:2001.07091*, 2020.

[17] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE international congress on big data (BigData congress)*. IEEE, 2017, pp. 557–564.

[18] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, and P. Rimba, "A taxonomy of blockchain-based systems for architecture design," in *2017 IEEE International Conference on Software Architecture (ICSA)*, 2017, pp. 243–252.

[19] "Ethereum. (n.d.)," 2019. [Online]. Available: https://www.ethereum.org/

[20] P. Hegedundefineds, "Towards analyzing the complexity landscape of solidity based ethereum smart contracts," in *Proceedings of the 1st International Workshop on Emerging Trends in Software Engineering for Blockchain*. New York, NY, USA: Association for Computing Machinery, 2018, p. 35–39. [Online]. Available: https://doi.org/10.1145/3194113.3194119

[21] M. C. Stefano Za, Monica Drăgoicea, "Blockchain technology as an enabler of service systems: A structured literature review bt - exploring services science," *Exploring Services Science*, pp. 12–23, 2017. [Online]. Available: https://doi.org/10.1007/978-3-319-56925-3

[22] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, vol. 36, pp. 55–81, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0736585318306324

[23] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey," *Int. J. Web Grid Serv.*, vol. 14, pp. 352–375, 2018.

[24] A. Satybaldy, M. Nowostawski, and J. Ellingsen, "Self-sovereign identity systems," 2019.

[25] M. S. Ferdous, F. Chowdhury, and M. O. Alassafi, "In search of self-sovereign identity leveraging blockchain technology," *IEEE Access*, vol. 7, pp. 103 059–103 079, 2019.

[26] L. Sislian and A. Jaegler, "Linkage of blockchain to enterprise resource planning systems for improving sustainable performance," *Business Strategy and the Environment*, 2021.

[27] P. Brody, "How blockchain is revolutionizing supply chain management," *Digitalist Magazine*, pp. 1–7, 2017.

[28] A. Shahaab, C. Hewage, and I. Khan, "Preventing spoliation of evidence with blockchain: A perspective from south asia," in *2021 The 3rd International Conference on Blockchain Technology*, 2021, pp. 45–52.

[29] M. Liu, J. Shang, P. Liu, Y. Shi, and M. Wang, "Videochain: trusted video surveillance based on blockchain for campus," in *International conference on cloud computing and security*. Springer, 2018, pp. 48–58.

[30] P. Agrawal, P. S. Anjana, and S. Peri, "Dehide: Deep learning-based hybrid model to detect fake news using blockchain," in *International Conference on Distributed Computing and Networking 2021*, 2021, pp. 245–246.

[31] S. Paul, J. I. Joy, S. Sarker, S. Ahmed, A. K. Das *et al.*, "Fake news detection in social media using blockchain," in *2019 7th International Conference on Smart Computing & Communications (ICSCC)*. IEEE, 2019, pp. 1–5.

[32] A. Qayyum, J. Qadir, M. U. Janjua, and F. Sher, "Using blockchain to rein in the new post-truth world and check the spread of fake news," *IT Professional*, vol. 21, no. 4, pp. 16–24, 2019.

[33] T. W. Jing and R. K. Murugesan, "A theoretical framework to build trust and prevent fake news in social media using blockchain," in *International conference of reliable information and communication technology*. Springer, 2018, pp. 955–962.

[34] G. Zhang, X. Zhang, M. Bilal, W. Dou, X. Xu, and J. J. Rodrigues, "Identifying fraud in medical insurance based on blockchain and deep learning," *Future Generation Computer Systems*, vol. 130, pp. 140–154, 2022.

[35] G. Saldamli, V. Reddy, K. S. Bojja, M. K. Gururaja, Y. Doddaveerappa, and L. Tawalbeh, "Health care insurance fraud detection using blockchain," in *2020 Seventh International Conference on Software Defined Systems (SDS)*. IEEE, 2020, pp. 145–152.

[36] J. Gera, A. R. Palakayala, V. K. K. Rejeti, and T. Anusha, "Blockchain technology for fraudulent practices in insurance claim process," in *2020 5th International Conference on Communication and Electronics Systems (ICCES)*. IEEE, 2020, pp. 1068–1075.

[37] X. Wang, L. Feng, H. Zhang, C. Lyu, L. Wang, and Y. You, "Human resource information management model based on blockchain technology," in *2017 IEEE symposium on service-oriented system engineering (SOSE)*. IEEE, 2017, pp. 168–173.

[38] N. N. Pokrovskaia, V. A. Spivak, and S. O. Snisarenko, "Developing global qualification-competencies ledger on blockchain platform," in *2018 XVII Russian Scientific and Practical Conference on Planning and Teaching Engineering Staff for the Industrial and Economic Complex of the Region (PTES)*. IEEE, 2018, pp. 209–212.

[39] M. M. H. Onik, M. H. Miraz, and C.-S. Kim, "A recruitment and human resource management technique using blockchain technology for industry 4.0," in *Smart Cities Symposium 2018*. IET, 2018, pp. 1–6.

[40] A. Pinna and S. Ibba, "A blockchain-based decentralized system for proper handling of temporary employment contracts," in *Science and information conference*. Springer, 2018, pp. 1231–1243.

[41] R. Bosri, A. R. Uzzal, A. Al Omar, A. T. Hasan, and M. Z. A. Bhuiyan, "Towards a privacy-preserving voting system through blockchain technologies," in *2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*. IEEE, 2019, pp. 602–608.

[42] S. T. Alvi, M. N. Uddin, L. Islam, and S. Ahamed, "A privacy-aware digital voting system employing blockchain and smart contracts," in *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*. IEEE, 2020, pp. 1–6.

[43] M. A. Tasnim, A. A. Omar, M. S. Rahman, M. Bhuiyan, and Z. Alam, "Crab: Blockchain based criminal record management system," in *International conference on security, privacy and anonymity in computation, communication and storage*. Springer, 2018, pp. 294–303.

[44] N. D. Khan, C. Chrysostomou, and B. Nazir, "Smart fir: securing e-fir data through blockchain within smart cities," in *2020 IEEE 91st vehicular technology conference (VTC2020-Spring)*. IEEE, 2020, pp. 1–5.

[45] I. Hingorani, R. Khara, D. Pomendkar, and N. Raul, "Police complaint management system using blockchain technology," in *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*. IEEE, 2020, pp. 1214–1219.

[46] A. Jain, S. Das, A. S. Kushwah, T. Rajora, and S. Saboo, "Blockchain-based criminal record database management," in *2021 Asian Conference on Innovation in Technology (ASIANCON)*. IEEE, 2021, pp. 1–5.

[47] J. Bacon, J. D. Michels, C. Millard, and J. Singh, "Blockchain demystified," *Queen Mary School of Law Legal Studies Research Paper*, no. 268, 2017.

[48] D. M. Vistro, M. S. Farooq, A. U. Rehman, and M. A. Khan, "Fraud prevention in taxation system of pakistan using blockchain technology," in *3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021)*. Atlantis Press, 2021, pp. 582–586.

[49] K. Wüst and A. Gervais, "Do you need a blockchain?" in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, 2018, pp. 45–54.

[50] Electron, https://www.electronjs.org/, 2021 (Retrieved June 5, 202).