

APPLICATION FOR ETHICAL APPROVAL

In order for research to result in benefit and minimise risk of harm, it must be conducted ethically.

The University follows the OECD Frascati manual definition of **research activity**: “creative work undertaken on a systematic basis in order to increase the stock of knowledge, including knowledge of man, culture and society, and the use of this stock of knowledge to devise new applications”. As such this covers activities undertaken by members of staff, postgraduate research students, and both taught postgraduate and undergraduate students working on dissertations/projects.

The individual undertaking the research activity is known as the “principal researcher”.

This form must be completed and approved prior to undertaking any research activity.

SECTION A: About You (Principal Researcher)

1	Full Name:	DEEP DESAI
2	Student Number:	2421862
3	Email address:	2421862@student.uwtsd.ac.uk
4	Programme of Study:	MSc Cybersecurity and Digital Forensics
5	Supervisor:	Mohamed Ghanem

SECTION B: Internal and External Ethical Guidance Materials

	Please list the core ethical guidance documents that have been referred to during the completion of this form (including any discipline-specific codes of research ethics, location-specific codes of research ethics, and also any specific ethical guidance relating to the proposed methodology). Please tick to confirm that your research proposal adheres to these codes and guidelines. You may add rows to this table if needed.	
1	UWTSD Research Ethics & Integrity Code of Practice	☒
2	UWTSD Research Data Management Policy	☒
3		☐
4		☐

SECTION C: Details of Research Activity

1	Indicative title:	Blockchain-Based Secure File Upload and Integrity Verification System using AES Encryption		
2	Proposed start date:	June 2026	Proposed end date:	September 2026
	Introduction to the Research (maximum 300 words in each section) Ensure that you write for a <u>Non-Specialist Audience</u> when outlining your response to the three points below: <i>Purpose of Research Activity</i>			

	• <i>Proposed Research Question</i> • <i>Aims of Research Activity</i> • <i>Objectives of Research Activity</i> Demonstrate, briefly, how Existing Research has informed the proposed activity and explain • <i>What the research activity will add to the body of knowledge</i> • <i>How it addresses an area of importance.</i>
3	Purpose of Research Activity The purpose of this research is to design, develop, and evaluate a secure file upload and integrity verification system using blockchain technology, AES encryption, and SHA-256 hashing. The study aims to enhance the confidentiality and integrity of digital files by ensuring that uploaded files are encrypted before storage and that any unauthorised modifications can be detected through cryptographic verification. The research will investigate how blockchain can be used to maintain tamper-resistant records of file integrity, while AES encryption protects sensitive data from unauthorised access. A prototype web-based application will be developed using the Flask framework to demonstrate secure file upload, encryption, storage, verification, and controlled tampering detection. The study is conducted for academic purposes as part of an MSc Cyber Security and Digital Forensics dissertation. No sensitive personal data, vulnerable participants, or human subject experiments will be involved. The research focuses on evaluating the effectiveness of the proposed security mechanisms in improving data protection within file management systems.
4	Research Question How can blockchain technology, AES encryption, and SHA-256 hashing be integrated to develop a secure file upload and integrity verification system that enhances data confidentiality and detects unauthorised file modifications?
5	Aims of Research Activity 1. Investigate the security challenges associated with traditional file upload and storage systems. 2. Design and develop a secure file upload system using AES encryption. 3. Implement a file integrity verification mechanism using SHA-256 hashing 4. Integrate blockchain technology for tamper-resistant record management 5. Evaluate the effectiveness of the proposed system through practical testing and controlled tampering simulations.
6	Objectives of Research Activity 1. Investigate security issues in traditional file storage systems. 2. Develop a secure file upload system using AES encryption. 3. Implement SHA-256 hashing for file integrity verification. 4. Integrate blockchain technology for tamper-resistant record management. 5. Evaluate the security and performance of the proposed system.
	Proposed data collection methods (maximum 600 words) Provide a brief summary of all the methods that may be used in the research activity to collect data, making it clear what specific techniques may be used. If methods other than those listed in this section are deemed appropriate later, additional ethical approval for those methods will be needed. You do not need to justify the methods here, but should instead describe how you intend to collect the data necessary for you to complete your project.
7	This research will collect data through a combination of literature review and system testing activities. The main aim is to develop and evaluate a secure file upload and integrity verification system using blockchain technology, AES encryption, and SHA-256 hashing. Since the project is technical in nature, no personal or sensitive information from human participants will be collected.

	The first method of data collection will be a review of existing academic and professional literature. Information will be gathered from peer-reviewed journal articles, conference papers, books, cybersecurity reports, and recognised standards. Sources such as IEEE Xplore, Springer, ScienceDirect, Google Scholar, NIST publications, and ISO standards will be used to understand current approaches to blockchain security, file encryption, integrity verification, and secure storage systems. This information will help establish the theoretical foundation of the research and identify gaps in existing studies. The second method will involve developing a prototype web application using the Flask framework. Data will be collected from the outputs generated by the system during development and testing. These outputs may include encrypted files, generated hash values, blockchain records, authentication results, upload logs, and verification results. The collected information will be used to assess whether the system performs as expected. To evaluate the effectiveness of the proposed solution, several functional tests will be carried out using sample files such as text documents, PDF files, and images. These files will be uploaded, encrypted, stored, verified, downloaded, and decrypted within the testing environment. The outcomes of these activities will be recorded and analysed to determine whether the system successfully protects file confidentiality and integrity. The research will also include integrity verification testing. SHA-256 hash values will be generated and compared at different stages of the file management process. In addition, controlled tampering tests may be performed by intentionally modifying stored files within the test environment. This will allow the researcher to examine whether the system can successfully detect unauthorised changes and report integrity violations. Performance-related information may also be collected during testing. This could include the time taken to upload files, perform encryption and decryption operations, generate hash values, and complete verification processes. These results will help evaluate the overall efficiency of the system. No interviews, surveys, questionnaires, focus groups, or observations involving human participants will be used in this study. All data will be obtained from academic sources and system-generated testing results. Therefore, the project presents minimal ethical risk and does not involve the collection of personal data. The collected data will be used solely for academic purposes and will contribute to the evaluation of the proposed blockchain-based secure file upload and integrity verification system.
--	---

SECTION D: Scope of Research Activity

	Will the research activity include:	YES	NO
1	Use of a questionnaire or similar research instrument?	☐	☒
2	Use of interviews?	☐	☒
3	Use of focus groups?	☐	☒
4	Use of participant diaries?	☐	☒
5	Use of video or audio recording?	☐	☒
6	Use of computer-generated log files?	☒	☐
7	Participant observation with their knowledge?	☐	☒
8	Participant observation without their knowledge?	☐	☒
9	Access to personal or confidential information without the participants' specific consent?	☐	☒

ETHICS FORM – COMPUTING STUDENTS ONLY

10	Administration of any questions, test stimuli, presentation that may be experienced as physically, mentally or emotionally harmful / offensive?	☐	☒
11	Performance of any acts which may cause embarrassment or affect self-esteem?	☐	☒
12	Investigation of participants involved in illegal activities?	☐	☒
13	Use of procedures that involve deception?	☐	☒
14	Administration of any substance, agent or placebo?	☐	☒
15	Working with live vertebrate animals?	☐	☒
16	Procedures that may have a negative impact on the environment?	☐	☒
17	Other primary data collection methods. Please indicate the type of data collection method(s) below.	☐	☒
	Details of any other primary data collection method: (this box should expand as you type)		

If you have ticked NO to every question then the research activity is (ethically) low risk and you may skip section E and continue to section F.

If YES to any question, then no research activity should be undertaken until full ethical approval has been obtained.

SECTION E: Intended Participants

	Who are the intended participants:	YES	NO
1	Students or staff at the University?	☐	☒
2	Adults (over the age of 18 and competent to give consent)?	☐	☒
3	Vulnerable adults?	☐	☒
4	Children and Young People under the age of 18? (Consent from Parent, Carer or Guardian will be required)	☐	☒
5	Prisoners?	☐	☒
6	Young offenders?	☐	☒
7	Those who could be considered to have a particularly dependent relationship with the investigator or a gatekeeper?	☐	☒
8	People engaged in illegal activities?	☐	☒
9	Others. Please indicate the participants below, and specifically any group who may be unable to give consent.	☐	☒
	Details of any other participant groups:		

	Participant numbers and source Provide an estimate of the expected number of participants. How will you identify participants and how will they be recruited?	
10	How many participants are expected?	N/A
11	Who will the participants be?	N/A

12	How will you identify the participants?	N/A
----	---	-----

	Information for participants:	YES	NO	N/A
13	Will you describe the main research procedures to participants in advance, so that they are informed about what to expect?	☐	☐	☒
14	Will you tell participants that their participation is voluntary?	☐	☐	☒
15	Will you obtain written consent for participation?	☐	☐	☒
16	Will you explain to participants that refusal to participate in the research will not affect their treatment or education (if relevant)?	☐	☐	☒
17	If the research is observational, will you ask participants for their consent to being observed?	☐	☐	☒
18	Will you tell participants that they may withdraw from the research at any time and for any reason?	☐	☐	☒
19	With questionnaires, will you give participants the option of omitting questions they do not want to answer?	☐	☐	☒
20	Will you tell participants that their data will be treated with full confidentiality and that, if published, it will not be identifiable as theirs?	☐	☐	☒
21	Will you debrief participants at the end of their participation, in a way appropriate to the type of research undertaken?	☐	☐	☒
22	If NO to any of above questions, please give an explanation			
	You should be able to tick YES for all of these questions. If not, then explain why not in this box. N/A			

	Information for participants:	YES	NO	N/A
24	Will participants be paid?	☐	☐	☒
25	Is specialist electrical or other equipment to be used with participants?	☐	☐	☒
26	Are there any financial or other interests to the investigator or University arising from this study?	☐	☐	☒
27	Will the research activity involve deliberately misleading participants in any way, or the partial or full concealment of the specific study aims?	☐	☐	☒
28	If YES to any question, please provide full details			
	You should be able to tick NO for most of these questions. For any cases that you have ticked YES then provide details in this box. If you are using cameras/voice recorders to record interviews then please state that in this box. N/A			

SECTION F: Anticipated Risks

	Outline any anticipated risks that may adversely affect any of the participants, the researchers and/or the University, and the steps that will be taken to address them.	
1	Risks to participants For example: sector-specific health & safety, emotional distress, financial disclosure, physical harm, transfer of personal data, sensitive organisational information. If you have identified in section D that there are no participants then enter N/A and go skip to question 3.	
	Risk to participants: There are always risks. Do not write N/A unless you have no participants.	How you will mitigate the risk to participants:

ETHICS FORM – COMPUTING STUDENTS ONLY

	N/A – This research does not involve human participants. The study is based on literature review, system development, and technical testing using non-sensitive sample files. Therefore, there are no identified risks relating to participant health and safety, emotional distress, financial disclosure, physical harm, personal data transfer, or sensitive organisational information.	
2	If research activity may include sensitive, embarrassing or upsetting topics (e.g. sexual activity, drug use) or issues likely to disclose information requiring further action (e.g. criminal activity), give details of the procedures to deal with these issues, including any support/advice (e.g. helpline numbers) to be offered to participants. Note that where applicable, consent procedures should make it clear that if something potentially or actually illegal is discovered in the course of a project, it may need to be disclosed to the proper authorities	
	N/A – This research does not involve human participants, interviews, questionnaires, surveys, or discussions relating to sensitive, embarrassing, or upsetting topics. The study focuses on the development and evaluation of a blockchain-based secure file upload and integrity verification system using technical testing and literature review. No personal, confidential, or sensitive participant information will be collected. Therefore, no additional support procedures, safeguarding measures, or disclosure procedures are required.	
3	Risks to the investigator For example: personal health & safety, physical harm, emotional distress, risk of accusation of harm/impropriety, conflict of interest	
	Risk to the investigator: There are always risks. Do not write NA. The risks to the researcher are considered minimal. The research primarily involves a literature review, software development, and system testing within a controlled computing environment. There is no anticipated risk of physical harm, personal safety concerns, or direct interaction with human participants. Potential risks may include minor eye strain, fatigue, or discomfort associated with prolonged computer use during software development, testing, and documentation activities. These risks will be managed through regular breaks, appropriate workstation setup, and adherence to standard health and safety practices.	How you will mitigate the risk to the investigator: The research does not involve sensitive personal data, confidential organisational information, or activities that could create a conflict of interest. Furthermore, all testing will be conducted using non-sensitive sample files within a secure development environment, reducing the risk of data breaches or unauthorised access. Overall, the project presents a low level of risk to the researcher and no significant ethical, physical, or psychological concerns have been identified.
4	University/institutional risks For example: adverse publicity, financial loss, data protection	
	Risk to the University: There are always risks. Do not write NA. The risks to the University are considered minimal. This research is conducted solely for academic purposes and involves the development and evaluation of a blockchain-based secure file upload and integrity verification system within a controlled testing environment. No personal data from participants will be collected, processed, or stored during the research. All testing will be performed using non-sensitive sample files created specifically for the	How you will mitigate the risk to the University: The project does not involve external organisations, commercial partnerships, financial transactions, or activities that could result in financial loss to the University. In addition, the research does not involve controversial, illegal, or high-risk activities that could create adverse publicity or reputational damage. Appropriate cybersecurity and data management practices will be followed throughout the project to ensure that all

ETHICS FORM – COMPUTING STUDENTS ONLY

	project. Therefore, the risk of data protection breaches or unauthorised disclosure of personal information is very low.	research materials, system outputs, and documentation are stored securely and used only for academic purposes. Overall, no significant institutional, financial, legal, reputational, or data protection risks have been identified.
5	Environmental risks For example: accidental spillage of pollutants, damage to local ecosystems	
	Risk to the environment: The research is not expected to create any environmental risks. The project involves literature review, software development, system testing, and evaluation activities conducted using computer systems in a controlled environment. No hazardous materials, chemicals, pollutants, or physical substances will be used during the research. The study does not involve fieldwork, laboratory experiments, or activities that could affect local ecosystems, wildlife, water sources, or the natural environment.	<i>How you will mitigate the risk to environment:</i> The only environmental impact is the normal use of computing resources and electricity required for software development, testing, and documentation, which is considered negligible and comparable to standard academic activities.

SECTION G: Feedback, Consent and Confidentiality

If you have identified in section D that there are no participants then enter skip this section and continue to section H.

1	Feedback What de-briefing and feedback will be provided to participants, how will this be done and when?
	You don't need to email your participants with your final report. A good alternative is to set up an email address that they will be able to contact for further details or results. N/A – This research does not involve human participants, interviews, surveys, questionnaires, or focus groups. Therefore, no debriefing or participant feedback procedures are required.
2	Informed consent Describe the arrangements to inform potential participants, before providing consent, of what is involved in participating. Describe the arrangements for participants to provide full consent before data collection begins. If gaining consent in this way is inappropriate, explain how consent will be obtained and recorded in accordance with prevailing data protection legislation.
	If you are using a paper questionnaire then you should have the participants sign an appropriate consent form. These forms will count as personal data and should be noted as such in section J. If you are using an online questionnaire, then you should have a screen before the questions start that acts as a consent form, informing participants that by clicking on the NEXT button they are providing consent. N/A – This research does not involve human participants, interviews, questionnaires, surveys, focus groups, or observation activities. Therefore, informed consent from participants is not required.
3	Confidentiality / Anonymity Set out how anonymity of participants and confidentiality will be ensured in any outputs. If anonymity is not being offered, explain why this is the case.
	Do not collect names unless you really need them. Do not name participants or organisations in any research publications (including the thesis) without their explicit permission.

ETHICS FORM – COMPUTING STUDENTS ONLY

	N/A – This research does not involve human participants and therefore no participant anonymity or confidentiality issues arise.
--	---

SECTION H: Data Protection and Storage

	Does the research activity involve personal data (as defined by the General Data Protection Regulation 2016 “GDPR” and the Data Protection Act 2018 “DPA”)?	YES	NO
1	“Personal data” means any information relating to an identified or identifiable natural person (‘data subject’). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Any video or audio recordings of participants is considered to be personal data.	☐	☒
	If YES, provide a description of the data and explain why this data needs to be collected:		
2	This includes audio/video data of participants, but can also include IP addresses and usernames. Names, addresses and emails also count, as do consent forms. N/A – No personal or identifiable data will be collected during this research. The study is based on literature review, software development, and system testing using non-sensitive sample files. Therefore, the collection of personal data is not required to achieve the research objectives.		
	Does it involve special category data (as defined by the GDPR)?	YES	NO
3	“Special category data” means sensitive personal data consisting of information as to the data subjects’ – (a) racial or ethnic origin, (b) political opinions, (c) religious beliefs or other beliefs of a similar nature, (d) membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), (e) physical or mental health or condition, (f) sexual life, (g) genetics, (h) biometric data (as used for ID purposes),	☐	☒
	If YES, provide a description of the special category data and explain why this data needs to be collected:		
4	What counts as ‘sensitive’ will differ between cultures. Any information on behaviour that is not in accordance with cultural norms would count as sensitive personal data. N/A – This research will not collect, process, or store any special category personal data. The study focuses on literature review, software development, and technical testing of a blockchain-based secure file upload and integrity verification system. No information relating to health, ethnicity, religion, political opinions, biometric data, sexual orientation, or other special category data will be required for the research.		

	Will data from the research activity (collected data, drafts of the thesis, or materials for publication) be stored in any of the following ways?	YES	NO
5	Manual files (i.e. in paper form)?	☐	☒
6	University computers?	☒	☐
7	Private company computers?	☐	☒
8	Home or other personal computers?	☒	☐

ETHICS FORM – COMPUTING STUDENTS ONLY

9	Laptop computers/ CDs/ Portable disk-drives/ memory sticks?	☒	☐
10	“Cloud” storage or websites?	☒	☐
11	Other – specify:	☐	☒
12	For all stored data, explain the measures in place to ensure the security of the data collected, data confidentiality, including details of backup procedures, password protection, encryption, anonymisation and pseudonymisation:		
	All data generated and used during this research will be stored securely and used solely for academic purposes. The research does not involve the collection of personal or sensitive participant data. The data used in the study will primarily consist of academic literature, system-generated outputs, test files, encryption results, hash values, blockchain records, and performance evaluation data. All project files, source code, documentation, and research materials will be stored on a password-protected personal computer accessible only to the researcher. Backup copies of important files will be maintained using secure storage locations, including encrypted local backups and approved cloud storage services where appropriate. To enhance data security, the developed system incorporates AES encryption to protect uploaded files and SHA-256 hashing to support integrity verification. Access to the application is restricted through user authentication mechanisms, ensuring that only authorised users can access system functions. As no personal data will be collected, anonymisation and pseudonymisation procedures are not required. However, any testing data used within the project will consist of non-sensitive sample files and will not contain identifiable personal information. Any system logs, test results, screenshots, or evaluation outputs included in the dissertation will be reviewed to ensure that no confidential information is disclosed. All research data will be retained in accordance with University guidelines and will be securely deleted when no longer required for academic purposes. These measures will help ensure data confidentiality, integrity, availability, and protection throughout the research process.		

	Data Protection		
	Will the research activity involve any of the following activities:	YES	NO
13	Electronic transfer of data in any form?	☒	☐
14	Sharing of data with others at the University outside of the immediate research team?	☐	☒
15	Sharing of data with other organisations?	☐	☒
16	Export of data outside the UK or importing of data from outside the UK?	☒	☐
17	Use of personal addresses, postcodes, faxes, emails or telephone numbers?	☐	☒
18	Publication of data that might allow identification of individuals?	☐	☒
19	If YES to any question, please provide full details, explaining how this will be conducted in accordance with the GDPR and Data Protection Act (2018) (and/or any international equivalent):		
	This research does not involve the collection of personal data or special category data from participants. The study is based on literature review, software development, and technical testing using non-sensitive sample files. Any research materials, system outputs, source code, and documentation will be stored securely on password-protected devices and used solely for academic purposes. The project will comply with the principles of the UK GDPR and the Data Protection Act (2018), including secure storage, restricted access, data minimisation, and appropriate data retention practices. No personal information will be shared with third parties.		

ETHICS FORM – COMPUTING STUDENTS ONLY

20	List all who will have access to the data generated by the research activity:	
	Researcher (Deep Desai) – Full access to all project files, source code, testing data, documentation, and research outputs. Dissertation Supervisor – Access to relevant research documents, progress reports, dissertation drafts, and final submission for academic supervision and assessment purposes. University Assessors/Examiners – Access to the final dissertation, project report, and supporting materials submitted for academic assessment.	
21	List who will have control of, and act as custodian(s) for, data generated by the research activity:	
	The primary custodian and controller of the research data will be the researcher (Deep Desai). The researcher will be responsible for the collection, storage, management, security, backup, and appropriate disposal of all research-related data. The dissertation supervisor may have access to relevant research materials, drafts, and project outputs for academic supervision purposes but will not act as the primary data custodian.	
22	Give details of data storage arrangements, including security measures in place to protect the data, where data will be stored, how long for, and in what form.	
	All research data will be stored on a password-protected computer and backed up using secure cloud storage. Data will include source code, test files, blockchain records, and dissertation documents. Access will be limited to the researcher and academic supervisor. All data will be stored electronically and retained in accordance with University requirements before being securely deleted	
22	Confirm that you have read the UWTSD guidance on data management (see https://www.uwttd.ac.uk/library/research-data-management/)	☒
23	Confirm that you are aware that you need to keep all data until after your research has completed or the end of your funding	☒

SECTION I: Use of AI tools

Use of generative AI and other AI-based tools		YES	NO	N/A
There are a number of ethical issues relating to the use of generative AI and other AI-based tools, including data security, output bias, and output errors. In general you should assume that any generative AI or other AI-based tool that you pay to use is more secure and accurate than one which is free to use.				
Will the research use AI tools to do any of the following:				
1	Capture data?	☐	☒	☐
2	Generate and/or edit text?	☐	☒	☐
3	Generate graphics?	☐	☒	☐
4	Generate video?	☐	☒	☐
5	Generate sound/music?	☐	☒	☐
6	Generate code?	☐	☒	☐
7	Generate synthetic data?	☐	☒	☐
8	Analyse data?	☐	☒	☐
9	Analyse personal or sensitive data?	☐	☒	☐

ETHICS FORM – COMPUTING STUDENTS ONLY

10	Classify data?	☐	☒	☐
11	Do you intend to use the free version of any AI tools?	☐	☒	☐
If you have answered YES to any of questions O1-O11, please provide justification detailing why this is necessary for the research.				
12	<i>N/A – No personal data, special category data, vulnerable participants, or other ethically sensitive information will be collected or processed as part of this research. Therefore, no additional justification is required.</i>			

SECTION J: Declaration

The information which I have provided is correct and complete to the best of my knowledge. I have attempted to identify any risks and issues related to the research activity and acknowledge my obligations and the rights of the participants. In submitting this application I hereby confirm that I undertake to ensure that the above named research activity will meet the University's Research Ethics and Integrity Code of Practice which is published on the website: https://www.uwtsd.ac.uk/research/research-ethics/			
1	Signature of applicant:	DEEP DESAI	Date: 9TH August 2026
2	Supervisor:	Mohamed Ghanem	Date:
3	Signature:		9th August 2026