

Research Project Proposal

Development of Mobile Applications (Apps) Security Standard (MASS)

Submitted by

**Dr. Sanjeev Singh
Institute of Informatics & Communication
University of Delhi South Campus
New Delhi – 110 021**

In Collaboration with

K-Grid Knowledge Ventures Pvt. Ltd, Noida

Objectives

The project aims to carry out research on **Mobile Applications (Apps) Security Standard (MASS)**. The research will be carried out by IIC, UDSC and K-Grid Knowledge Ventures Pvt. Ltd. The project MASS will include

- (1) Define the mobile apps security category, which can be used to evaluate the mobile app security vulnerability, and
- (2) Define the mobile app security certification framework, which can be used to validate the mobile app implantation standard procedures.

PROJECT DESCRIPTION

Mobile applications are software applications designed to run primarily on smartphones, tablets, and pocket PCs. They are distributed by application market places and are specific to the Operating System (OS) of the mobile devices. The four most popular mobile application distribution market places are

- (1) Apple App Store,
- (2) Google Play,
- (3) BlackBerry App World, and
- (4) Windows Phone Store.

The Apple App Store provides applications for Apple's IOS-based iPhones and iPads, the Google Play for Android-based OS mobile devices, the BlackBerry App World for the Research In Motion's BlackBerry mobile devices and Windows Phone store for Microsoft's Mobile Phones, tablets, and pocket PCs. Since 2009, thousands of applications that can be installed and used on mobile devices have flooded these application market places. These mobile applications have evolved from their initial use as productivity, entertainment, and utility applications. Now users, customers, and employees are conducting their day-to-day business transactions on mobile devices. Businesses need to develop and provide mobile applications to their employees and customers to keep pace with the changing business and consumer landscape. However, these mobile applications have also introduced major security concerns for businesses and enterprises as hackers and bad actors can exploit them to steal and harm customers and businesses.

Mobile application security protects an organization from potential threats, leveraging the customer-facing mobile applications an organization develops as attack vectors. Mobile application security covers mobile applications, communication between mobile applications and backend infrastructure, backend infrastructure, and the associated activities, processes,

and work streams used to design, test, develop, deploy, operate, and maintain these technologies.

Evolving Threat Landscape of Mobile Security Worldwide

In the asian region and around the world, an increasing number of businesses, consumers, and employees are using mobile applications to conduct daily business transactions using mobile devices due to availability, ease, and accessibility of mobile ecosystems. A recent survey of consumers indicates that 83 percent of the population in cities uses smartphones to conduct business or enterprise transactions. In addition, 64 percent of those surveyed use mobile devices to conduct banking. However, the survey also revealed that one in three people have experienced cybercrime in the past 12 months and close to 50 percent of the people surveyed lack a basic understanding of mobile security and proper cyber hygiene. This survey data indicates that the stakes are high when it comes to mobile security and risk levels are only going to elevate as more and more businesses enable mobile application-based transactions to attract a new generation of consumers.

While consumer confidence and awareness is a key driver for addressing mobile security, the stakes are even higher for businesses and enterprises. They are the ultimate victims of cybercrime that could occur from breach in mobile application security. This threat is especially high for financial institutions. Regulators and banks are starting to address this quickly evolving threat landscape facing mobile applications.

The Open Web Application Security Project (OWASP) is an organization that has focused on improving the security of software in general and recently emphasizing mobile application security. As illustrated in figure 1, OWASP has released the top 10 mobile application vulnerabilities that organizations must address when it comes to providing security for mobile applications. Any one of these vulnerabilities can cause serious damage to a financial institution via loss of data, reputation, and consumer confidence—all of which lead directly and indirectly to financial losses.

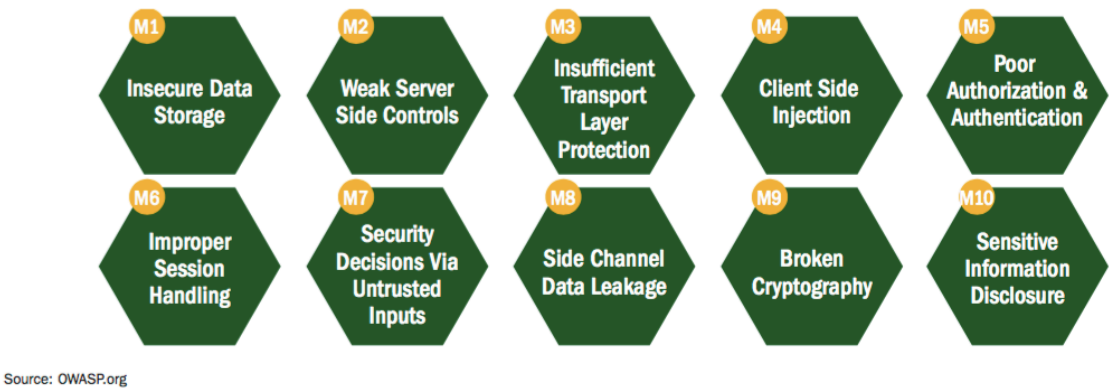


Figure 1: Top 10 mobile application vulnerabilities

Identifying Vulnerabilities and Malicious Mobile Exploits

The project aims to study on defining the vulnerabilities further and identifying the potential mobile security exploits that could harm or damage a business. Several potential exploits are shown in figure 2. Our mobile security experts understand the implications these exploits can have on business and consumer confidence and how organizations can best protect themselves against them.

Any one of these exploits can lead to loss of private data; loss of usernames, passwords, and personal identification numbers (PIN); unauthorized access to private, business, and financial data; and theft and fraud. For example, a stolen device that may have unencrypted data stored on the device could easily give a bad actor access to a person's private data. A malware on a mobile device could easily forward username and passwords of a banking mobile application to hackers that could result in loss of financial data. Man-in-the-middle attacks were a major threat to web-based and online transactions, but now, they are increasingly more common on mobile devices. Controls such as two factor authentication across same communication channels are helpless against a stolen device or a device with malicious malware. These sophisticated attacks to mobile applications are well orchestrated and must be defended against through a pragmatic and holistic approach to mobile application security.

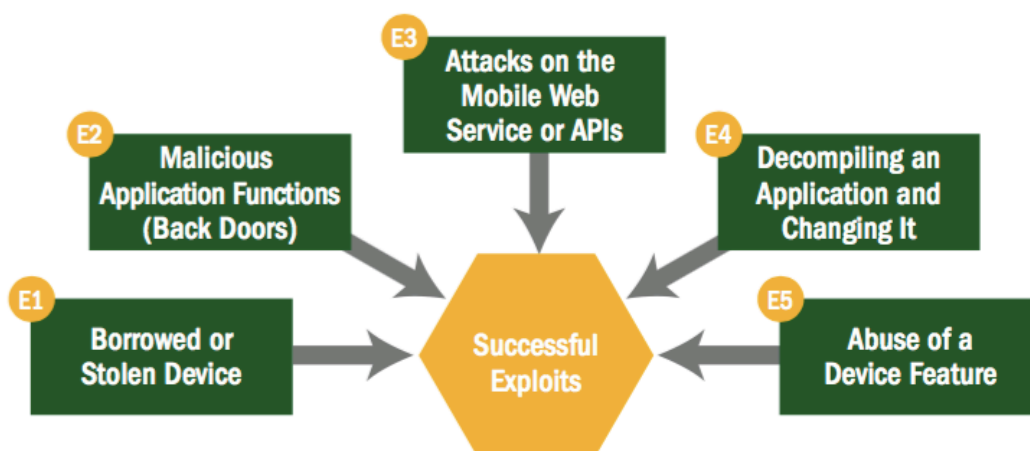


Figure 2: Key potential exploits

Approach to Mobile Security

Effective mobile application security program starts with addressing three primary pillars of mobile application security:

(1) secure mobile applications,

(2) secure mobile data transmission, and

(3) secure mobile backend infrastructure

All three must be assessed and addressed across all aspects of people, processes, and technology dimensions. Our mobile application security professionals help organizations

- **Develop an understanding of holistic solution and approaches to providing mobile application security standard framework**
- **Utilize the same basic principles that apply to web and online security to mobile application security**

The approach is to assess and develop framework for across mobile applications, mobile data transmission, and mobile backend infrastructure addresses the following categories:

- **Vulnerabilities.** Identify vulnerabilities based on risk profiles
- **Relevant Security Controls.** Identify and implement security controls
- **Best Security Practices.** Identify relevant security best practices and institutionalize them
- **Useful Frameworks and Standards.** Identify and adapt where relevant the various articles, tools, frameworks, and international standards.

FUNDING

2.1 K-Grid will pay a total amount of Rs.13,56,000/- (Rupees Thirteen Lakhs fifty six thousand only). Payment shall be made by K-Grids according to the following schedule.

- i. 50% payment on approval and startup of the project
- ii. Remaining 50% payment will be released after first report and utilization certificate

S No	Item	Amount in Rupees
A	Duration: One Year	
1	Manpower: 3 Project Researchers (@ Rs 30,000 pm consolidated)	10,80,000
3	Contingencies (miscellaneous and sundry expenses including stationary, printing and travel)	50,000
	Sub Total	11,30,000
4	University Overhead Charges (@20 %)	2,26,000
	Total	13,56,000

The IIC, UDSC will raise the demand note/ funding request on K – Grid for the payments due and payable under the provisions of terms and conditions (as per the annexure A).

Annexure A

K – GRID, IIC, UDSC RESEARCH AGREEMENT

This Agreement is entered into effective this 15th day of June 2016 (the “Effective Date”) by and between K – Grid Knowledge Ventures Pvt. Ltd (**K - Grid**) having its principal office in 498, Sector 28, Noida, and the **IIC, UDSC**, with its principal address at Institute of Informatics and Communication, University of Delhi South Campus.

WHEREAS, the research contemplated by this Agreement is of mutual interest and benefit to the K - Grid (hereafter named **K - Grid**) and to the IIC, UDSC, and will further the instructional and research objectives of University in a manner consistent with its status as a non-profit, tax-exempt educational institution and should derive benefits for both the K - Grid and the University.

NOW, THEREFORE, in consideration of the premises and the mutual covenants contained herein, the parties here to agree:

ARTICLE 1 - RESEARCH WORK

1.1 The University will use its best efforts to perform research in accordance with the project description, funding and special conditions specified in Appendix A (the "Project").

1.2 The Project shall be conducted under the direction of the Principal Investigator(s) as specified in Appendix A. A named Principal Investigator can be replaced only upon the prior written consent of K - Grid.

ARTICLE 2 - REPORTS AND CONFERENCES

2.1 Reports and research deliverables developed on Project, as specified in Appendix A, will be submitted by the University, through the Principal Investigator for Project.

2.2 During the term of the Project, representatives of the University may meet the representatives of K - Grid at times and places mutually agreed upon by the Principal Investigator and K - Grid to discuss the progress and results, as well as ongoing plans, or changes therein (as provided in writing), of the Project to be performed here under. Such discussions may also be held by teleconferencing as mutually agreed upon by the Principal Investigator and the K - Grid.

ARTICLE 3 - PUBLICATIONS

3.1 The Publication of the research results is of fundamental importance to the University. The University must, therefore, be permitted to publish the research results in recognized scientific journals, conferences and conference proceedings. A copy of any proposed publication (herein after called "Manuscript") will be submitted to the K - Grid at least thirty (30) days in advance of the submission for publication to assure that:

- (a) No confidential or proprietary information, as defined in Article 7.1, is contained in the Manuscript. Such material will be removed from the Manuscript before it is submitted for publication;
- (b) The Manuscript does not disclose inventions intended for inclusion in the patent applications yet to be filed. Such material will be removed from the Manuscript before it is submitted for publication or the publication will be delayed for a period of time not to exceed six (6) months to allow for time to prepare and file patent applications.
- (c) With stipulations as mentioned in (a) and (b), the permission to publish the research results will be given by the K - Grid within a reasonable period not exceeding 6 months

ARTICLE 4 - INTELLECTUAL PROPERTY

4.1 The "K - Grid Intellectual Property" means: (i) all products and processes of inventions, improvements and discoveries, whether or not patentable, prior to the Project which are conceived solely by one or more employees of the K - Grid and/or, (ii) all products and processes of inventions, improvements and discoveries, whether or not patentable, relating to the Project which are conceived solely by one or more employees of the University and/or jointly by employees of the University and the K - Grid, and which refers to patent(s) owned or assigned to the K - Grid, or which are developed as a result of the K - Grid's Confidential Information, as defined in Article 7.1. The K - Grid Intellectual Property will be owned solely by the K - Grid, subject to the license granted in Article 6.4, and will not otherwise be subject to the terms and conditions of this Agreement.

4.2 The "University Intellectual Property" means all products and processes of inventions, improvements and discoveries which are conceived by one or more employees of the University before the course of the Project and is needed under the Project and not covered under Article 4.1. The University Intellectual Property will be owned solely by the University and will be subject to the terms and conditions of this Agreement.

4.3 The "Joint Intellectual Property" means all products and processes of inventions, improvements and discoveries which are conceived by one or more employees of the University and one or more employees of the K - Grid in the course of the Project and not covered under Article 4.1 and 4.2. Such Joint Intellectual Property will be either owned by the Party who bears all the costs relating to the filing, prosecuting and maintaining of patent applications in its own name as explained under Articles 4.4 and 4.5 herein below (or) will be jointly owned by the University and the K - Grid as detailed in Article 4.7 and will be subject to the terms and conditions of this Agreement or other Agreement(s) to be entered into between the parties exclusively for this purpose.

4.4 Upon disclosure of a Joint Intellectual Property conceived and/or reduced to practice in the course of a Project, the K - Grid will notify the University in writing within thirty (30) days whether or not the K - Grid wishes to exploit the Joint Intellectual Property. If Parties decide by mutual consent that the K - Grid shall own and exploit the said Intellectual Property in its own name, the K - Grid will prepare a patent application or other application for protection of such Joint Intellectual Property. The K - Grid will promptly prepare, file and prosecute such patent applications in India, U.S. and foreign counterparts and in other countries selected by K - Grid in the K - Grid's name. The K - Grid will bear all costs incurred in connection with such preparation, filing, prosecution and maintenance of U.S. and foreign counterparts directed to the said Joint Intellectual Property developed in connection with the Project hereof and the Intellectual Property rights of such Joint IP shall be owned by the K - Grid exclusively. The University will cooperate with the K - Grid to assure that such application(s) will cover, to the best of their knowledge, all items of commercial interest and importance. While the K - Grid will be responsible for making decisions regarding the scope and content of application(s) to be filed and prosecution thereof, the University will be given an opportunity to review and provide input thereto. The K - Grid will keep the University advised as to all developments with respect to such application(s) and will promptly supply to the University copies of all papers received and filed in connection with the prosecution thereof in sufficient time for the University to comment thereon. Each party shall obtain an assignment from its inventor-employees in order to establish such party's ownership interest in the patent applications and patents issuing thereon.

4.5 If the K - Grid elects not to exercise its option as set forth in Article 5.1 hereof or decides not to exploit the Joint Intellectual Property or file patent applications or prosecute Joint Intellectual Property as set forth in Article 4.4 above, it shall inform the University, so that the University may elect to file patent application for the Joint Intellectual Property in its name in accordance with Article 4.4 above and maintain any protection issuing thereon in the India, U.S. and in any foreign country at University's sole expense, and the K - Grid will have no further rights to the respective patent applications or issued patents. The University also reserves the right to file applications in countries not selected by K - Grid.

4.6 In the above cases, the declining Party shall retain its rights of use as detailed under Article 6 below, but shall lose its rights of ownership and exploitation in respect of the Joint Intellectual Property.

4.7 If the parties decide, by mutual agreement to file, prosecute and maintain IP rights protection of the Joint Intellectual property, in their joint names, Parties shall equally bear all costs resulting from such activities and the Parties shall enter into a Joint Ownership Agreement which will include inter alia equal rights of ownership, use and rights of exploitation.

ARTICLE 5 - GRANT OF RIGHTS

5.1 The University grants the K - Grid the first option to obtain either:

(a) A exclusive, fully paid up, license to make, have made, use, sell, offer for sale and import the University Intellectual Property related to the Project, with a right to grant sublicense of the same

scope to any of K - Grid's Affiliates, but not to sublicense to any other third party. For the purpose of this Agreement “Affiliate” means a corporation, partnership, or venture at least 50% of the voting interests or ownership of which is controlled by or controlling the K - Grid or having a common control; or

(b) An exclusive, fully paid up license to make, have made, use, sell, offer for sale and import the University Intellectual Property related to the Project or the University's share of the Joint Intellectual Property arising out of the K – Grid ed research project with the right to sublicense.

5.2 If the K - Grid wishes to exercise either option as specified in Article 5.1 (a) and (b) above, the University and the K - Grid will enter into a confirmatory license agreement within six months from exercise of the option. The parties shall mutually agree the fully paid up fee in a confirmatory license agreement (Articles 6.1 and 6.2), which shall not exceed INR Ten Lakhs.

5.3 If the K - Grid exercises its option under Article 6.1 (b) to obtain an exclusive license, the University will have an irrevocable, royalty free, nonexclusive and non-assignable license to use all patentable or patented products, materials, processes, and all other University Intellectual Property and Joint Intellectual Property, for research and educational purposes but not for commercial purposes.

5.4 The K - Grid grants the University an irrevocable, royalty-free, nonexclusive, and non-assignable license to any K - Grid Intellectual Property for which one or more employees of University were inventors, for research and educational purposes, but not for commercial purposes.

5.5 No right to use a Party’s Intellectual Property (Pre-existing materials of respective parties described under Article 4.1 and 4.2) granted by one party to the other party independently of the Joint Intellectual Property. Any sub-license or third parties agreement will oblige the parties concerned to abide by such a limitation.

5.6 A Party shall not pledge, assign, sell or otherwise dispose of its interest in the Joint Intellectual Property to the third parties without the other Party’s prior written consent.

5.7 An assignment within a conglomerate (to parent company and affiliates of K - Grid or in a case of Change in Control of K - Grid is permissible (“Change in Control of K - Grid” means (a) consolidation or merger of the K - Grid or its parent company or affiliate, with or into any entity, (b) sale, transfer or other disposition of all or substantially all of the assets of any of the foregoing; (c) acquisition by any entity, or group of entities acting in concert, of beneficial ownership of 50% or more of the outstanding voting securities or partnership interests of any of the foregoing. Any Change of Control in Applied will not affect the IP rights of the University.

5.8 Any change in status of “K - Grid” by merger, acquisition or otherwise will not affect the IP rights of the University.

ARTICLE 6 - CONFIDENTIAL INFORMATION:

6.1 "Confidential Information" means:

(a) any information disclosed to the University by the K - Grid in written or recorded form and clearly marked as confidential;

(b) any information disclosed to the University by the K - Grid or ally or by visual inspection that, at the time given, is stated to be confidential, and is confirmed in writing within thirty (30) days; and

(c) any confidential or proprietary data directly related to the K - Grid product or process.

6.2 The Principal Investigator, IIC, UDSC agree to keep Confidential Information confidential for a period of five (5) years from the date given to the University, not to disclose in any form to any third party, and to only disclose to the University employees who have a need to know, and to use such Confidential Information only for the purposes of this Agreement.

6.3 The obligations, as stated in Article 6.2, will not apply to information which:

(a) is at the time of receipt public knowledge, or after receipt becomes public knowledge through no act of omission on the part of the University;

(b) was known to the University, as shown by written records, prior to disclosure by the K - Grid; or

(c) is received by the University from a third party who did not obtain the information from the K - Grid.

6.4 From time to time, the University may need to provide Applied with confidential or proprietary information. The parties agree to negotiate on case by case basis non-disclosure agreements which are specific to the information the University intends on disclosing.

ARTICLE 7 - TERM AND TERMINATION

7.1 This Agreement will continue for a period of one (1) years from the Effective Date unless sooner terminated in accordance with the provisions of this Article. The parties hereto may extend the term of this Agreement in writing for additional periods as desired on mutually acceptable terms and conditions.

7.2 Either party may terminate this Agreement without cause if written notice of termination is given to the other party at least sixty (60) days prior to the proposed termination date.

7.3 Termination of this Agreement by either party for any reason will not affect the rights and obligations of the parties accrued prior to the effective date of termination. Articles 3, 4, 5, 6, 7, 9, 10, 11, 12, 13 and 14 shall survive termination to the extent applicable.

7.4 Any undisclosed Joint Intellectual Property conceived or reduced to practice prior to termination of Agreement shall be treated in the same manner as if no such termination has taken place.

ARTICLE 8 - INDEPENDENT CONTRACTOR

In the performance of all services here under:

8.1 The University will be deemed to be and will be an independent research and development contractor and, as such, no employees or staff of the University will be entitled to any benefits applicable to the employees of the K - Grid;

8.2 Neither party is authorized or empowered to act as an agent for the other for any purpose and will not on behalf of the other enter into any contract, warranty, or representation as to any matter. Neither party will be bound by the acts or conduct of the other party.

ARTICLE 9 - INDEMNITY

9.1 University will indemnify, hold harmless and defend the K - Grid against any and all claims, demands, actions, liability, expenses and fees ("Claims"), related to or arising out of any deliverables provided by the University to the K - Grid resulting from the Project (the "Deliverables"). Notwithstanding to the foregoing, University shall not be liable for any Claims above, if such Claims arise as a result of: (a) University having followed a design or instruction furnished by the K - Grid in writing; (b) use of the Deliverables in a manner contrary to the written specifications of University provided to the K - Grid prior to the Claim arising; (c) association or combination of the Deliverable with any other equipment, programs or materials not supplied by the University

The University will indemnify, hold harmless and defend the K - Grid, and its officers, directors, trustees, employees and agent (the "K - Grid's Indemnified Parties") against any and all Claims related to or arising out of the University's failure to comply with such regulatory requirements, provided that each of the K - Grid's Indemnified Parties provides prompt notice of any Claims and provides information and assistance as reasonably requested by University.

ARTICLE 10 - GOVERNING LAW AND DISPUTE RESOLUTION

11.1 This Agreement will be governed and construed in accordance with the Laws of India.

Dispute Resolution: Any dispute/difference and/or claim arising out of or in connection with this Agreement shall be resolved amicably between the authorized representatives of both the parties failing which such dispute/difference and/or claim shall be resolved by arbitration of a sole arbitrator to be nominated and appointed by mutual consent of both the parties. In the event of arbitrator so appointed is unable to proceed with the arbitration proceeding for any reason whatsoever, both parties shall, by mutual consent, appoint another arbitrator in his place, who

shall become entitled to proceed with the arbitration proceeding from the state at which it was left by his predecessor. The arbitration proceeding shall be governed by the provisions of the Arbitration & Conciliation Act 1996 and / or any statutory amendments thereof. The award passed by the arbitrator shall be final and binding on the parties. The venue of arbitration shall be at Delhi.

ARTICLE 11 - ASSIGNMENT

11.1 This Agreement may not be assigned by either party without the prior written consent of the other party hereto, provided however, that the K - Grid may assign this Agreement to an affiliate as defined in Articles 5.1 and 5.7.

ARTICLE 12 - NOTICES

12.1 Notices and communications will be addressed to the party to receive such notice or communications at the address given below, or such other address as may hereafter be designated by notice in writing:

If to the K - Grid
For Contractual Matters:

If to the K - Grid
For Technical Matters

If to the University
For Contractual Matters:

If to the University
For Technical Matters:


ARTICLE 13-GENERAL

13.1 This instrument, including Appendix A, contains the entire agreement between the parties with respect to the subject matter hereof, and any representation, promise or condition in connection therewith not incorporated herein will not be binding on either party. If any term of this Agreement is held invalid or unenforceable, such term will be considered omitted from this Agreement and will not affect the validity or enforceability of the rest of this Agreement. No modification to the terms of this Agreement will be valid unless made in writing and signed by authorized representatives of the parties.

13.2 Paragraph headings used in the Agreement are for reference only and shall not be used or relied upon in the interpretation of this Agreement.

13.3 The foregoing has been agreed to and accepted by the parties hereto and their authorized signatories have accordingly appended their signatures below which shall include their successors in office and assigns.

AR(F)/4259
22/8/16


22/8/16

IN WITNESS WHEREOF, this Agreement has been executed in duplicate by the Parties authorized representatives as of the day and year first above written.

Signature of the Authorized Signatory
Signed for and on behalf of

K – Grid Knowledge Ventures Pvt. Ltd

By: 

Name: Sanjay Sharma

Title: CEO, K-Grid


Signature of the Authorized Signatory
Signed for and on behalf of
IIC, UDSC

By: 

Name: Dr. Sanjeev Singh, IIC, UDSC

Title: Principal Investigator

Forwarded to AR (Fin) UDSC.


22/08/2016
In Charge
Institute of Informatics & Communication
University of Delhi South Campus
Benito Juarez Road, New Delhi-110021

Delhi University


29/8/16

By: _____

Name: निदेशक / Director
दिल्ली विश्वविद्यालय, दक्षिण परिसर
University of Delhi, South Campus
नई दिल्ली-110021
New Delhi-110021

Title: _____