IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.7, Special Issue.1, Jan 2019 E-ISSN: 2347-2693

A Study on Different Applications of M-governance and its Security

D. Banerjee[1*], S. K. Karforma [2]

[1]Department of Computer Science, St. Xavier's College Burdwan, Burdwan, India
[2] Department of Computer Science, The University of Burdwan, Burdwan, India

*Corresponding Author: debduttab13@gmail.com, Tel.: +09051384495

Available online at: www.ijcseonline.org

***Abstract*—** Mobile governance (m-governance) provides all the government services in a convenient manner. The proper establishment of e-governance has a great impact on the initiatives taken for m-governance. M-governance can be presumed as an extension of e-governance. Mobile computing and different communication technology are used for delivering different government services and for accessing information from both the central and state governments. M-governance provides greater flexibility to all the users of different domains. Security is the most important issue in today's world. This paper gives an overview of the architecture and framework of m-governance as well as various applications of government initiatives on a mobile platform with different aspects of providing security to all these projects. These mobile applications can be successfully instigated and sustained only if the m-governance framework can implement the optimum security structure. It can convince all the participants about its authenticity, integrity, acceptability, as it is solely responsible for securing all the public information from unauthorized access, by using different security techniques like encryption, digital signature, digital certificates, watermarking etc.

***Keywords*—**M-governance Framework, Security, Risks, Mobile Applications

I. INTRODUCTION

M-governance, a sub-domain of e-governance, is the application of mobile technologies to provide e-governance services to the citizens as well as to make the whole system more efficient, effective, fast, transparent, responsive and liable for information exchanging and different transactions within government, between government and government agencies. Core users of m-governance are government, citizens, and businesses sectors [1].

It can be considered as one enhanced application of Information and Communication Technology (ICT) for making available various government services to each and every one for different information inter-change, both way communications, various kinds of transactions through mobile technology. This system can be recognized as the incorporation of various stand-alone systems and services as well as to run different back-office processes and interactions within the entire government framework.
It is now sprouting on four extents [2]–

a) Transforming services of e-governance directly to the mobile platform
b) Offering access to different government application through smartphones for all the personnel of different sectors
c) Facilitating smart functioning to all the back end and front end users
d) Delivering government services to the citizens anytime, anywhere.

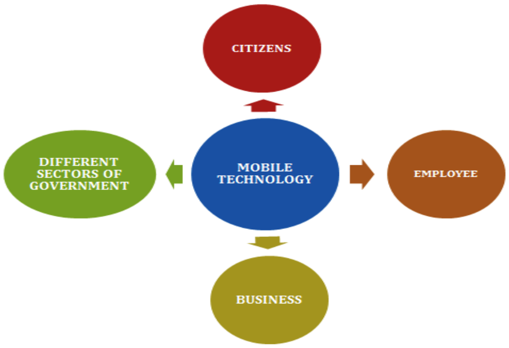

Fig-1: Different Users of M-Governance

To ensure acceptance and performance of the m-governance framework in time bound manner, now the government is trying to develop Mobile Service Delivery Gateway (MSDG) that is the basic infrastructure for enabling the availability of public services in smartphone through different platforms like android, windows and java applets.

Nowadays mobile phone appears as a channel for information broadcasting in government services. Thus through m-governance, government services turn out to be more convenient, well-organized, transparent and useful manner. Hence through m-governance, citizens of India can circumvent the need for traditional physical networks for communications and collaboration. With the advancement of ICT, e-governance has transformed to m-governance.

There are about 650 million mobile phone users in India now, and just over 337 million of them have a smartphone i.e., more than a quarter of the population, are using a smartphone in 2018, according to the latest forecast and it will be increased day by day. Thus, nowadays, the rate of using smart mobile phones is also increasing drastically as shown in the following graph [3]

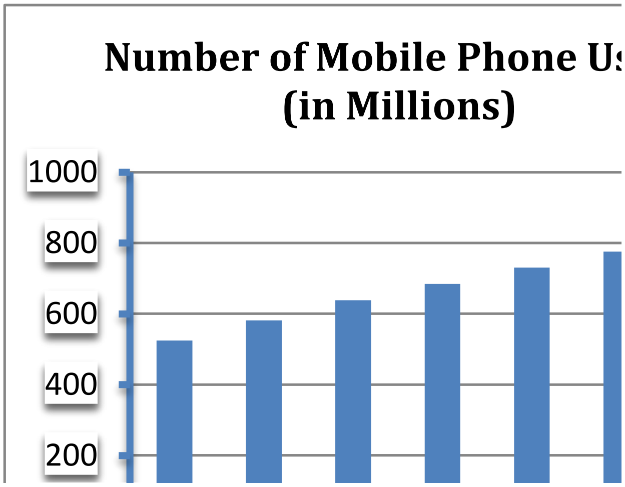

Fig-2: Increasing rate of mobile phone user

II. Characteristics of M-Governance

1. Greater Accessibility: The main characteristic of m-governance is availing government services at anytime and anywhere as there are no limitations for time and place of using smartphones.

2. Real-Time Monitoring: M-Governance confirms better amenity of the existing services like bill payment, online form submission, reservation or ticket booking for travelling and tourism purposes, checking information by enabling easy retrieval of information anytime, anywhere for the all the citizens and bring together all the services of the government.

3. Effective Adaptability: Policies and working procedures in all the sectors (Education, Health, Agriculture, Finance, Weather forecasting, Bill payment, Travel and Tourism, Judicial and legal systems) of government are changing in a daily basis. Effective adaptability of m-governance is an advantage in the harshly changing system.

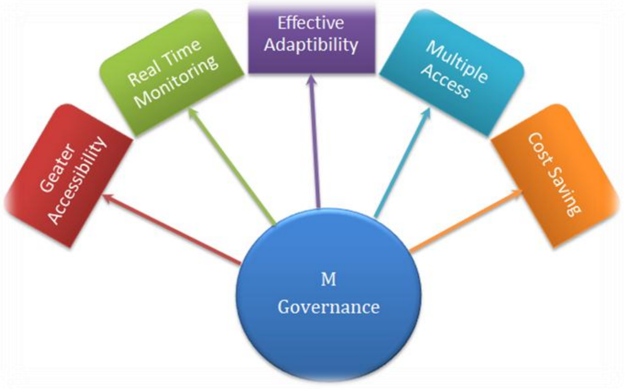

Fig-3: Characteristics of M-Governance

4. Multiple Accesses: M-governance affords a powerful and transformational capacity to both extend access to existing services, and expands the delivery of new services for increasing active involvement of the public in the various government projects.

5. Cost Saving: Availing mobile technologies for accessing all the services anywhere and anytime is not even costlier nowadays as the interfaces are becoming more user-friendly day by day and maintenance cost is minimal too.

III. Architetural Framework of M-Governance

Different users of m-governance systems access server from mobile platforms via internet connections provided by the different service providers. End to end security is needed for making safe the whole system. The following architecture is employed for the execution of the m-governance system.

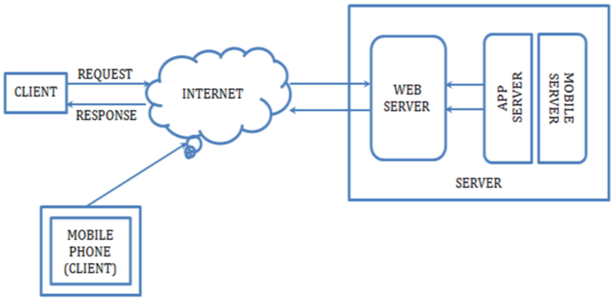

Fig-4: Basic Architecture of M-Governance

IV. Models of M- Governance

The core architecture of m-governance framework is based on the following four models [4].

1. mG2C: This front office application is used for delivering interface to make communication between government-to-citizen. It helps citizens to stay up-to-date on current government movements, as well as people can be directly connected with the government by requesting services, making different transactions, enquiring questions, giving feedback by making report problems and by requesting emergency assistance.

2. **mG2B:** This is a front office application, used for arranging different dealings between government-to-business agencies by providing information regarding policies, protocols, license, agreements, sanctioning different demands, taxes paid as well as give assistance and sponsorship for small and medium enterprises and business development.

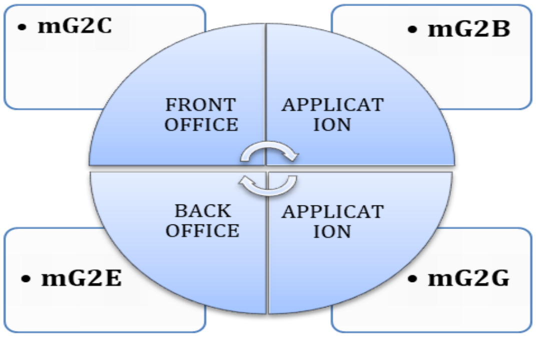

Fig-5: Different models of M-governance

3. **mG2G:** This back office application is used for establishing connections between government-to-government, i.e., a collaboration between different sectors of government as well as between central and local government agencies so that the whole system can progress as a single unit**.**

4. **mG2E:** This back office application is used for providing the interface between government-to-employees through some government aided tools, training, and data access authorization to their employees for their day to day works to improve the quality of service to the citizens. Thus organizational effectiveness and efficiency are maximized with the limited resources by enabling real-time access to enter, retrieve and share data from rural and remote locations too through mobile.

V. DIFFERENT INITITIVES OF M-GOVERNANCE

Some Mobile Applications for Different Fields of M-Governance:

Various m-governance facilities are analyzed for different domains like AADHAAR, agriculture, Indian post, health, judiciary, language, m-learning, e-taxation, e-commerce, transport, municipality and corporation, electoral with the special emphasis on security aspects [5].

1. **Mobile Seva** enables the integration of the mobile platform with the common e-Governance infrastructure consisting of State Data Centers (SDCs), State Wide Area Networks (SWANs), State and National Service Delivery Gateways (SSDGs/NSDG) by providing an well-equipped platform for all the sectors of Government and public agencies throughout the country using SMS (Short Message Service), CBS (Cell Broadcasting Service), USSD (Unstructured Supplementary Service Data), IVRS (Interactive Voice Response System) and Mobile Internet apps.

Different security techniques like visual cryptography, pattern recognition, biometric authentication are accepted for restricting unauthorized access of personal mobile by locking mobile screens through password or pin, different pattern matching, fingerprints recognition or face detection method. These procedures are already instigated in different mobile platforms like android technology and windows.

2. M-Aadhaar is an official mobile application developed by UIDAI (Unique Identification Authority of India) to run an interface for the aadhaar card holders to carry their personal information alike Name, Photograph, Date of Birth, Gender and Address along with the biometrics information for fingerprint matching and iris recognition as linked with their Aadhaar Number.

One can open the pdf (Portable Document Format) file of the e-Aadhaar card by inputting a combination of the first four letters of the name written in CAPITALS (Name as mentioned in the Aadhaar card) and Year of Birth (in YYYY format) as e-Aadhaar card password or e Aadhaar card PDF password. UIDAI has made the process of obtaining Aadhaar Virtual ID (VID), a revocable 16-digit random number mapped with Aadhaar details, easier to ensure the protection of personal information o Aadhaar data. UIDAI motivates to use VID and has recently added a new feature of a "Masked Aadhaar Card". Therefore the application can be made secure from illegal accesses. [6]

3. **UMANG** (Unified Mobile Application for New-age Governance) brings a single platform to all the populations of India, for availing multiple government services by installing one application.

4. **BHIM** (Bharat Interface for Money) is a mobile app developed by NPCI (National Payments Corporation of India) grounded on the UPI (Unified Payment Interface) 2.0 for making e-payments directly through banks. As part of

the 2016 Indian Banknote Demonetizations and drive towards a cashless transaction, BHIM is launched.

Anyone can make direct bank payments to anyone on UPI using their UPI ID or scanning their QR code (Quick Response Code) with the BHIM application. One can also request money through the app from a UPI ID. With this option, while making payment through scanning QR, the user will get additional security in the form of signed QR / intent. Security issues related to altering QR as well as having non-verified entities will be reduced by introducing the signed QR. Thus authenticity will be ensured of the receiver and will be informed if the QR is not secured. The transaction must be done faster as application password will not be required in case of signed intent.

5. **Hamraaz,** Android-based mobile application that has been developed solely for serving soldiers of Indian Army not for civilians by the technical team of Army (Adjutant General's Branch (MP-8)) for communication of their service and pay related information to them on their mobile phones. The latest version uploaded on 18 Sep 2018 caters for a major change in user verification scheme for different security concerns and other implementation problems related to use of Aadhaar No. [7]

6. **Kisan Suvidha Mobile Application** is designed for providing a common platform to the farmers as well as to the agriculture stakeholder, available in Hindi, English, Punjabi, Tamil and Gujarati Language. The farmers can get information regarding the weather forecast, dealer’s details, current market status, techniques for protecting plants from pest, weed, insects, and diseases, and professional advice through kisan call centre from technical experts.
Special security techniques are not required for this kind of general use applications.

7. **Swachhata Application** is an official application to use citizen involvement providing direct connections for resolving all the Swachha Bharat grievances [8].

8. **M-Passport Seva** is designed primarily for getting passport related information like the fee structure, application status, contact information and other general information. It is trying to be updated more so that the public can submit online applications.

9. **Mera Aspatal** is an ICT based Patient Satisfaction System (PSS) used for public and empanelled private hospitals to allow the patients for sharing views on the quality of experience in a public healthcare facility through proper feedback keeping system.

10. **Meri Sadak** is a versatile mobile application to empower residents to give their critical feedback with respect to the pace of work, nature of work.

11. **RAS** (Rapid Assessment System) mobile application is an initiative to investigate the given feedbacks and generating knowledge out of them which in turn can help to improve the future experience in availing public services.
These mobile applications face different kinds of risks caused by hackers. Hackers perform different active or passive attacks exploring the weakness of TCP/IP protocol and mobile OS.

Different security techniques are needed for building trust in the mind of all the participants of m-governance. At present internet hackers or intruders are either changing or modifying the data during unauthorized transactions from senders’ end or receivers’ end through mobile or computer. As a result, so far significant number of citizens is diffident to use smartphones or computers for financial transactions using a credit card or debit card details or net banking details, as well as some other confidential and important information like aadhaar card number, pan card number, biometric information.

To diminish above risks different security techniques may be applied; those are discussed in the next section.

VI. SECURITY IN M-GOVERNANCE

Data security is the process of keeping information safe and protected from unauthorized access, retrieval, modification, assessment or loss of information. There are many ways for keeping data secure including encryption, strong user verification and backup solutions [9].
The security services in the mobile platform can be distributed into three different levels.

- Root Level
- Infrastructure Level
- Application Platform Level

The **Root Level** security of mobile technology constitutes the security surveillance on cloud physical systems. This helps in observing the servers and technologies in the cloud infrastructure.
The **Infrastructure Level** controls the virtual machines in the cloud.
In the **Application Platform Level**, several activities such as user authentication, key validating etc. are carried out.
Different security techniques can be adopted to provide protection to the m-governance system in these three levels; some of them include [10]

1. **Encryption:** Encryption is the process of encrypting a message in such a way that an authorized receiver can only decrypt the message with the key provided by the instigator to the recipients only.
   In an encryption system, the projected information, referred to as plaintext, is encrypted using an encryption algorithm by generating cypher text that can be read

only if decrypted with the key like ATM pin or AADHAAR No.

Modern mobile technology uses RSA based algorithms, IDEA and ElGamal encryption algorithm to encrypt and decrypt messages. RSA is an asymmetric cryptographic algorithm with two different keys. Data Encryption Standard (DES) algorithm is commonly used in ATM machines (to encrypt PINs) and is utilized in UNIX password encryption. Triple DES or 3DES has replaced the older versions as a more secure method of encryption, as it encrypts data three times and uses a different key for at least one of the versions [11].

Thus we can restrict unauthorized access of confidential messages from the government side to others i.e. for mG2G, mG2C and mG2B models.

2. **Digital Signature:** A digital signature is a mathematical practice used for validating the authenticity of a message, software or digital document. Different algorithms are used to verify the integrity of the signed data and the identity of the signatory [12].

   Electronic documents like e-receipts, bank statements and other documents related to different government transactions contain the digital signature for limiting unauthorized access.

   Rabin Cryptosystem, ECDSA and ElGamal Algorithms can be used for implementing the digital signature system in mobile platforms.
3. **Digital Certificate:** A digital certificate, an electronic document, which contains the digital signature of the concerned specialist and then drags together a public key with an identity. This identity can be used to verify whether a public key belongs to a particular person or entity or not [13].

   PKI **(**Public Key Infrastructure) is used to generate, distribute, save and revoke digital certificates by using public-key encryption with a set of predefined rules, guidelines, and approaches [14].

   A digital certificate is allotted by a Certification Authority (CA). Now TCS and NIC are served this role in India. The commonly used digital certificate standard is X.509.
4. **Visual Cryptography:** Visual cryptography is a special cryptographic technique which allows graphical information (pictures, text, etc.) to be encrypted. It can be easily decrypted by the human vision only for the correct key images [15].

   This practice can be used for validating the user access to retrieve, modify, read or open some confidential files like different uploaded ID cards, documents of M-Aadhaar, different e-receipts, downloaded documents or for making some financial transactions.
5. **Biometric Authentication**: Biometrics is implemented through human body measurements and calculations through the metrics related to different human characteristics. Biometric authentication is a form of identification and access control. Visual cryptography can be used for protecting biometric originals so that decryption can be possible without any complex computations.

   Nowadays, this method is rapidly used for applying security in the banking industry. It can be used for numerous operations of all the models of m-governance.
6. **Watermarking:** Watermarking is the practice of keeping digital information hidden in a carrier signal to validate the integrity of the carrier signal as well as to show the individuality of its owners [16].

   This process can be used by keeping digital information hidden for the users of mG2B, mG2C model and mG2G models like for issuing different certificates related to different government transactions , receipts etc.
7. **Steganography:** Steganography is the process of embedding secret messages within an ordinary message to hide it from the outside world. The extractions of the hidden message will be possible at its requirement only. It functions by swapping bits of not so important data in common files like graphics, sound, text [17].
8. **Mobile Cloud Computing (MCC) Security:** Cloud Computing service provides all the facilities to the users of smartphones through SaaS, PaaS, IaaS approaches.

   The mobile cloud computing security covers various phases and monitors all the components in the cloud. It includes the privacy and integrity of stored data, the availability of the cloud services, the allocations of the resources as well as the authentication of the users and devices with running applications. [18]

VII. CONCLUSION

Due to the growing rate of availability, flexibility and user-friendliness of mobile technology, governments are promoting and using smartphones for providing e-governance services. Accordingly, mobile phones are used as an effective tool to make a more active communication system between citizen-government. Day by day Government is taking initiatives to simulate different m-governance services to smooth out all the services provided to the citizen of India.

Hackers are also performing new practices rapidly for making various attacks on the systems. As a consequence different security skills are needed for securing the whole m-governance system.

VIII. FUTURE SCOPE

These risks and remedies of m-governance are also applicable in a similar type of services like m-learning, m-commerce, m-banking etc.

REFERENCES

[1] Sumanta Bhattacharya, Joyita Goswami (Ghosh), "*Study of E-Governance: The Attractive Way to Reach the Citizens*", IJCA Special Issue on "2nd National Conference- Computing, Communication and Sensor Network", CCSN, 2011.

[2] Dr Ashok Jain, Kiran Ranawat, "*M-Governance in India: Problems and Acceptability*", Imperial Journal of Interdisciplinary Research (IJIR), Vol-3, Issue-1, 2017

[3]https://www.statista.com/statistics/274658/forecast-of-mobile-phone-users-in-india/

[4] Mrs Vaishali Kadu1, Ms.Vijaya Mahesh Bagret2, Mr.Abhishek Verma, "*Transforming from e-Governance to M-Governance*", International Journal of Advanced Research in Computer and Communication Engineering" Vol. 4, Issue 2, February 2015.

[5] https://www.2thepoint.in/m-governance-brief/

[6]http://vikaspedia.in/e-governance/mobile-governance/m-governance-in-india

[7]https://apps.mgov.gov.in/descp.do?appid=1430&param=app.password%20of%20hamraazSolution

[8] Miss. M. Debora, "*M-Governance in India: Issues and Initiatives*", International Journal of Computer & Mathematical Sciences, IJCMS, ISSN 2347 – 8527, Volume 7, Issue 2, February 2018

[9] Kumar D, Dr N. Panchanatham "*A case study on Cyber Security in E-Governance*", International Research Journal of Engineering and Technology (IRJET), Volume: 02 Issue: 08 | Nov-2015

[10] Abhishek Roy, Sunil Karforma, "*A Survey on E-Governance Security*", International Journal Of Computer Engineering And Computer Applications Issn 0974- 4983.

[11] A Roy, S Banik, S Karforma, J Pattanayak, "*Object-oriented modelling of IDEA for E-governance security*", Proceedings of International Conference on Computing and Systems 2010, 263-269

[12] Prof. Sunil Karforma and Dr Abhisek Roy, "*A survey on digital signatures and its applications*", J. of Comp. and I.T. Vol. 3(1&2), 45-69 (2012).

[13] Nikhilesh Barik & Dr Sunil Karforma, *"A Study on Efficient Digital Signature Scheme for E-Governance Security",* Global Journal of Computer Science and Technology, Volume 12, Issue 3, Version 1.0, February 2012

[14] Vishal R. Pancholi, Dr Bhadresh P. Patel, Dr Dilendra Hiran, "*A Study on Importance of Digital Signature for E-Governance Schemes",*
IJIRST –International Journal for Innovative Research in Science & Technology| Volume 4 | Issue 10 | March 2018, ISSN (online): 2349-6010

[15] M.Suganya and Dr.S. Suganya, "*A Fingerprint Biometric Privacy Using Visual Cryptography* ", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056, Volume: 04 Issue: 04 | Apr -2017

[16] Soumendu Banerjee, Sunil Karforma, "*Object-Oriented Modeling for Authentication of Certificate in E-Learning Using Digital Watermarking*", International Journal of Advanced Research in Computer Science, Volume 8, Issue 8.

[17] Frank Y.Shih, "Digital watermarking and steganography: Fundamentals and techniques", CRC Press, London, New York

[18] M. Padma, M. Lakshmi Neelima, "Mobile Cloud Computing: Issues from a Security Perspective", IJCSMC, Vol. 3, Issue. 5, May 2014.

Authors Profile

Debdutta Banerjee has completed her Bachelors in Physics from the University of Burdwan, and her Masters in Computer Application (MCA) from the Bengal Institute of Technology, West Bengal University of Technology. She is currently working as Head in the Dept. of Computer Science at St. Xavier's College, Burdwan. Her research interests include Data Security, E-governance, E-Commerce, M-governance and Cloud Security.

Prof. Sunil Karforma has completed his Bachelors in Computer Science & Engineering, and his Masters in Computer Science & Engineering, from Jadavpur University. He received his Ph. D. in Computer Science from the University of Burdwan. He is presently Professor and Head of the Department of Computer Science at the University of Burdwan.His research interests include Network Security, E-Commerce, E-governance and Bioinformatics. He has published numerous papers in both national as well as international journals and conferences. He is serving as an editorial member and reviewer of several international reputed journals.