Formally Verified Secure and Scalable Mobile Governance Framework

[1]Saeed MushailKafeer Al Qarni, [2*]Mohammed AlShehri & [3]Shaik Shakeel Ahamad
[1]s5m5algarni@hotmail.com [2*]ma.alshehri@mu.edu.sa & [3]s.ahamad@mu.edu.sa
College of Computer and Information Sciences, Majmaah University, Majmaah 11952, Saudi Arabia

Summary
The number of smartphone users and their usage is in high rise [1]. So the future of electronic governance lies with smartphones for providing services to the citizens. Current literature in the realm of mobile governance is not robust, scalable and secure. Intruders target three areas for vital information they are Mobile Government Application (MGA), during the transit of messages, and Government Server. This paper overcomes these flaws and proposes a novel framework for secure mobile government. Our proposed protocol ensures all the security properties. The proposed protocol ensures security and freshness of the keys, the security of data at rest, and during transit are ensured and finally overcomes reverse-engineering attacks, Proposed protocol withstands all the known attacks as it is formally verified using BAN Logic.

Keywords: ***Mobile Government Application (MGA), Scalable, Robust, freshness of the keys, reverse engineering attacks, BAN Logic***

1. Background

The number of smartphone users and their usage is in high rise [1]. So the future of electronic governance lies with smartphones for providing services to the citizens. The use of Information and Communication Technologies (ICT) applications changed the way the government function [2]. The exponential development of wireless technologies also has a positive impact on the development of mobile governance [3]. As per the UN website, electronic government refers to the use of information and communication technologies (ICT) including Wide Area Networks, the Internet, cloud, and mobile computing" [4]. The mobile government is defined as a strategy and its implementation involving the utilization of wireless and smartphone technology, services, applications, and devices for improving benefits to the entities involved in electronic government, including citizens, businesses and all government establishments [7]. Mobile Government is defined as a strategy which uses mobile and wireless technology compared to the traditional wired electronic government services [5]. So, the mobile government helps in delivering services to the citizens at their respective locations [6]. The success of mobile government initiatives around the globe depends on citizen's satisfaction and security of the framework, but the existing mobile government initiatives in the literature are not secure as the citizen's credentials and information can be compromised. A secure mobile government framework needs to ensure Authentication, Integrity, Confidentiality, and Non-Repudiation properties. Mobile Government Applications (MGA) are replacing browser for providing services to the citizens using smartphones. Despite MGA's popularity, there are some genuine concerns that are pushing back, particularly the security of these services. A Mobile Government Application (MPA) runs on a smartphone and contains very important information related to citizens. Intruders target three areas to get important information. Following are the three areas that need to be addressed for a secure mobile government framework

i) Mobile Government Application (MGA)
ii) Data during the Transit
iii) Government Server

These assets belong to the citizen, Government, and during transit. So a secure mobile government framework needs to address the security of Mobile Government Application (MPA), messages exchanged during the transit and security at the Government server. We haven't found a mobile government framework that ensures security. Most of the works in the literature focus on e-governance framework. As per our knowledge, we are the first to propose a secure Mobile Government framework catering to the needs of the Mobile Government. Rao and Karoma [8, 9] proposed two different electronic governance schemes using digital certificates, and this solution is based on the smart card. These solutions have the following limitations

i) key management
ii) security and freshness of the keys are not achieved

*Corresponding Author: ma.alshehri@mu.edu.sa

iii) There is no clarity on how communication and application security is ensured.
iv) There is no clarity on how security is ensured at the government end.

Rao and Karoma [10] proposed a secure mechanism for electronic governance based on a smart card. This work uses Multipurpose Electronic Card (MEC). This solution has the following limitations

i) key management
ii) security and freshness of the keys are not achieved
iii) There is no clarity on how communication and application security is ensured.
iv) There is no clarity on how security is ensured at the government end.
v) Not scalable

The following are the contributions made

a) Proposes a secure, scalable and robust mobile governance framework.
b) A novel key management protocol is proposed in the realm of secure mobile governance framework.
c) Proposed framework ensures all the security properties.
d) The proposed protocol ensures security and freshness of the keys, overcomes reverse engineering, the security of data at rest, and during transit are ensured.
e) Our proposed protocol is verified successfully using BAN logic.
f) Proposed framework overcomes all the flaws in the existing literature.

The rest of the paper is organized as follows. Section 2 proposes a secure mobile government framework. Section 3 presents the formal verification using BAN logic, and Section 4 presents the Security analysis of our proposed system, Section 5 presents the comparative analysis of the protocol with related work. Finally, Section 6 concludes the paper.

2. Proposed Mobile Governance Framework

Citizen, Government, and Certifying Authority (CA) are the entities involved in mobile government ecosystem. Citizen (C) is the entity that uses government services with Mobile Government Applications (MGA) installed on their smartphones. Government (G) has a Trusted Platform Module (TPM), which plays an important role in key management. Certifying Authority (CA) is responsible for issuing certificates to all the entities involved in the system. A novel key management is proposed in our mobile government framework. Symmetric key is shared between the Mobile Government Applications (MGA) of the Citizen’s smartphone and the Government. CA verifies the authenticity of MGA. Citizen (C) and government server generates their own credentials and provides their proof of credentials to CA. CA issues certificates to the stakeholders in the ecosystem. Mobile Government server manages all the citizens’ accounts and shares symmetric keys with all the citizens. Application security and communication security are ensured in our proposed system which is very crucial for the success of Mobile Government system. Key management is very important success of Mobile Government system. Our proposed system updates the symmetric keys of all the MGA’s at regular intervals via OTA (Over The Air) thereby ensuring the security of the transmitted messages. Figure 1 depicts CA issuing X.509 Certificates to both Government and Citizen Entities.

Technical Architecture: There are three servers at the Government end, and they are Registration Server (RS) with the credential repository, Authentication Server (AS) with fraud management service, and Authorization Server (AZS) with identity directory. Registration Server (RS) with credential repository registers the citizens for government services after successful verification of their credentials. Authentication Server (AS) authenticates the credentials of the citizens to verify the identity of the citizens. It verifies the identity of the citizens by cross-checking with fraud management service if the verification is successful, it provides the services to the citizen. Authorization services to citizens are provided by the Authorization Server (AZS). AZS provides only to those citizens who are authorized to use that service. Authorization services are provided based on the policy of the government, and the roles of the identity are with the identity directory updated with the roles and permissions. Our proposed framework is scalable as mobile government has three different servers; they are Registration server, Authentication Server and Authorization Server.

TABLE I. NOTATIONS

Notation	Full-Form/Meaning
$SYYKEY_{GC}$	Symmetric Key Shared between Government (G) & Citizen (C)
CID	Identity of the Citizen (C)
T_C	Time Stamp generated by Citizen (C)
T_G	Time Stamp generated by the Government (G)
N_C	Nonce generated by Citizen (C)
N_G	Nonce generated by Government (G)
ACK	Acknowledgment
TID	Transaction ID
SERVICE	Service provided by
RS	Registration Server
AZS	Authorization Server
AS	Authentication Server
C	Citizen
G	Government

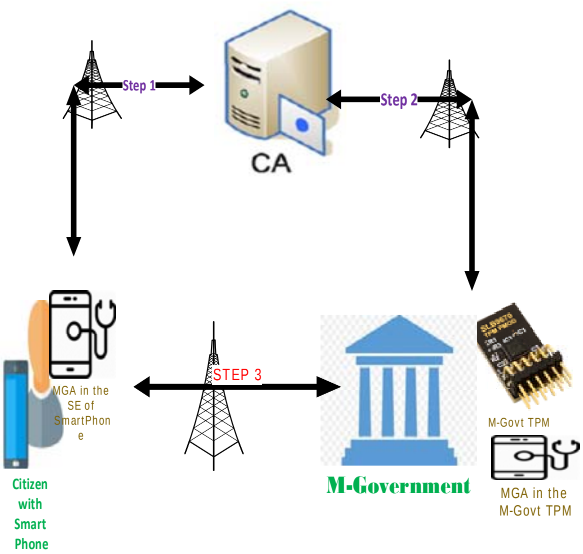

Fig. 1. CA issues X.509 Certificates to both Government and Citizen

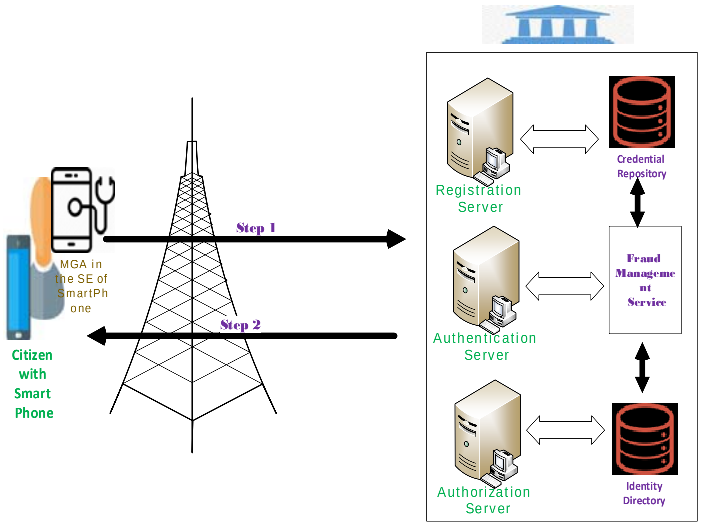

Fig. 2. Proposed Protocol in Mobile Government Framework

Our Proposed Protocol: There are two steps involved in our proposed protocol. Figure 2 depicts the steps involved in the proposed protocol in the mobile government framework.

$\mathbf{Step1}: \mathbf{C} \rightarrow \mathbf{G}: \{\mathbf{CID}, \mathbf{SERVICE}, \mathbf{N_C}, \mathbf{T_C}\}\mathbf{SYYKEY_{CG}}$

Step 1: Citizen (C) authenticates himself to the MGA by inserting the PIN. He fills the MGA with $\{\mathbf{CID}, \mathbf{SERVICE}, \mathbf{N_C}, \mathbf{T_C}\}$MGA encrypts the message with the symmetric key shared between himself and Government (G).

$\mathbf{Step2}: \mathbf{G} \rightarrow \mathbf{C}: \{\mathbf{CID}, \mathbf{SERVICE}, \mathbf{ACK}, \mathbf{TID}, \mathbf{N_G}, \mathbf{T_G}\}\mathbf{SYYKEY_{GC}}$

Step 2: Government (G) TPM receives the message and decrypts the message using the symmetric key shared between G and C. Government (G) verifies all the attributes in the message, if the verification is successful, it provides required services to the citizen.

3. Formal Verification

'E' is a set of entities containing {C, G, and CA}. These assumptions describe the public and private keys of the entities used to authenticate each other.

AS1. CA **believes** $(\forall E \in \{C, G, \text{and } CA\} \overset{K_e}{\mapsto} E)$ Certification Authority CA believes that all the entities have their public keys to communicate.

AS2. $E \in \{C, G \text{ and } CA\}$ **Sbelieves** $\overset{K_{ca}}{\mapsto} CA)$. All the stakeholders in the framework know the public key of the certification authority CA.

AS3.G believes freshness(N_C)& C believes freshness(N_G)

AS4. $T_C T_G$ are the timestamps generated Citizen and Government ensuring the **timeliness** of the messages exchanged.
AS5. ($\forall E, Q \in \{C, G, \text{and } CA\}$, E **believes** CA **controls** $\overset{K_{ca}}{\mapsto} Q$.
All the entities trusts CA.

Step 1: $\mathbf{C \rightarrow G: \{CID, SERVICE, N_C, T_C\}SYYKEY_{CG}}$

Government (G) receives $\{CID, SERVICE, N_C, T_C\}SYYKEY_{CG}$ from Citizen (C) and decrypts the message using $SYYKEY_{CG}$ and gets$\{CID, SERVICE, N_C, T_C\}$. So from the assumptions AS1 and AS 2
G **believes**$\{CID, SERVICE, N_C, T_C\}SYYKEY_{CG}$ ….Statement (1)
G verifies N_C, T_C from the message received and from the assumptions AS3 to AS5 it successfully verifies the timestamps and nonce….Statement (2)
From statements 1 & 2
G **believes**$\{CID, SERVICE, N_C, T_C\}$

Step2: $\mathbf{G \rightarrow C: \{CID, SERVICE, ACK, TID, N_G, T_G\}SYYKEY_{GC}}$

Citizen (C) receives $\{CID, SERVICE, ACK, TID, N_G, T_G\}SYYKEY_{GC}$from Government (G) and decrypts the message using $SYYKEY_{CG}$ and gets $\{CID, SERVICE, ACK, TID, N_G, T_G\}$. So from the assumptions AS1 and AS 2
C **believes** $\{CID, SERVICE, ACK, TID, N_G, T_G\}SYYKEY_{CG}$ ….Statement (3)
C verifies N_G, T_G from the message received and from the assumptions AS3 to AS5 it successfully verifies the timestamps and nonce….Statement (4)
From statements 3 & 4
C **believes**$\{CID, SERVICE, ACK, TID, N_G, T_G\}$

4. Security Analysis

Confidentiality: Messages are encrypted using the shared symmetric keys and the security is relied on continuously updating the keys at regular intervals Over The Air (OTA) thereby ensuring confidentiality of the messages.

Integrity: Our proposed protocol ensures the integrity of the messages at both application layer and communication layer, which is very important for the success of mobile government system.

Mutual Authentication: Mutual authentication property is ensured X.509 certificates, Government TPM and MGA establishes a secure exchange of messages (by encrypting the messages at the application layer) and communication layer using SSL/TLS.

Secrecy of the Keys: MGA of citizen (C) and the TPM at the Government shares a symmetric key and the symmetric key is updated at regular intervals thereby ensuring the security of the keys.

Replay Attacks: Encrypted messages using the shared symmetric keys, Nonce and timestamps plays crucial role in overcoming replay attacks.

Impersonation Attacks: Encrypted messages using the shared symmetric keys which are updated at regular intervals, Nonce and timestamps plays crucial role in overcoming impersonation attacks.

Man-In-The-Middle Attacks: Encrypted messages using the shared symmetric keys which are updated at regular intervals, Nonce and timestamps plays crucial role in overcoming Man-In-The-Middle attacks.

5. Comparative Analysis with Related Work

Table 2 compares our proposed protocol with the related works [8, 9 & 10] discussed in section 1, and we found that our proposed system ensures Mutual Authentication, Confidentiality, Authorization, and Accountability. Our proposed system ensures Freshness and Security of Keys, Application Security, and implements Defense in Depth. Proposed system Overcomes Reverse engineering attacks, Replay attacks, Impersonation attacks, Man-In-The-Middle Attack. In addition to these proposed systems ensures Security of the Data at Rest and during the Transit.

Protocols / Features	[8]	[9]	[10]	OURs
Mutual Authentication	Yes	Yes	Yes	Yes
Scalability	No	No	No	Yes
Confidentiality	Yes	Yes	Yes	Yes
Authorization	Yes	Yes	Yes	Yes
Accountability	Yes	No	No	Yes
Integrity	Yes	No	No	Yes
Freshness and Security of Keys	No	No	No	Yes
Application Security	No	No	No	Yes
Communication Security				
Defense in Depth	No	No	No	Yes
Overcomes Reverse engineering attacks	No	No	No	Yes
Replay attacks	Yes	Yes	Yes	Yes
Impersonation attacks	Yes	Yes	Yes	Yes
Man In The Middle Attack	Yes	Yes	Yes	Yes

Security of the Data at Rest	No	No	No	Yes
Security of the Data during Transit	No	No	No	Yes
Formal Verification	No	No	No	Yes

Table. 2: Comparative Analysis of our proposed work with related work

6. Conclusion

Electronic governance's future lies with smartphones in order to provide services to citizens. Existing literature in the area of mobile governance is not scalable, robust and secure as attackers target three areas for getting vital information they are Mobile Government Application (MGA), during the Transit of messages and Government Server. So we have addressed these limitations by proposing a novel framework for the secure mobile government as our proposed protocol ensures all the security properties and ensures security and freshness of the keys, overcomes reverse-engineering attacks, the security of data at rest and during transit are ensured, in addition to these proposed framework is scalable and robust which is very vital for the success of mobile governance. In addition to these our proposed protocol withstand all the known attacks as our proposed protocol has been successfully verified using BAN Logic.

References

[1] Mubarak S. Al-Mutairi. M-Government: Challenges and Key Success Factors – Saudi Arabia Case Study. pp 78-96

[2] Layne, K., & Lee, J. (2001). Developing fully functional e-government: A four stage model. *Government Information Quarterly*, *18*, 122–136. doi:10.1016/S0740-624X(01)00066-1

[3] Kakihara, M., & Sorensen, C. (2002). Mobility: An Extended Perspective. 35th Hawaii International Conference on System Sciences, Hawaii, USA.

[4] Easton, J. (2002). Going Wireless: transform your business with wireless mobile technology. USA: HarperCollins.

[5] Kushchu, I., & Kuscu, H. (2003). From e-government to m-government: Facing the Inevitable? In the proceeding of European Conference on e-government (ECEG 2003), Trinity College, Dublin.

[6] Goldstuck, A. (2004). Government Unplugged: Mobile and wireless technologies in the public service. Center for public services innovation, South Africa.

[7] Kushchu I (2007) Mobile government: an emerging direction in e-government. Mobile Government Consortium International, UK. IGI Publishing

[8] Roy A, Banik S, Karforma S (2011) Object oriented modelling of RSA digital signature in e-governance security. Int J Comput Eng Inf Technol 26:24–33

[9] Roy A, Karforma S (2012) Object oriented approach of digital certificate based e-governance mechanism. ACEEE Conf Proc Ser 3:3–4

[10] Roy A, Karforma S (2013) UML based modeling of ECDSA for secured and smart E-Governance system. In Computer Science and Information Technology (CS and IT-CSCP 2013), Proceedings of National Conference on Advancement of Computing in Engineering Research (ACER13) organized by Global Institute of Management and Technology, pp 207–222. doi:10.5121/csit.2013.3219

[11] Burrows, M., Abadi, M. and Needham, R. (1989) 'A logic of authentication', *Proceedings of the Royal Society of London A*, February, Vol. 426, pp.233–271, A preliminary version appearedas Digital Equipment Corporation Systems Research Center report No.39.

[12] Burrows, M., Abadi, M. and Needham, R. (1990) 'A logic of authentication', *ACM Transactions on Computer Systems*, Vol. 8, No. 1, pp.18–36.

Saeed MushailKafeer Al Qarniis currently ng his Master in Cybersecurity and Digital Forensics at College of Computer and Information Sciences, Majmaah University Majmaah, Saudi Arabia. His research areas include Network Security and Digital Forensics. He can be reached at s5m5algarni@hotmail.com

Dr. Mohammed Abdulrahman Alshehri is currently working as a Dean and Associate Professor at the College of Computer and Information Sciences, Majmaah University Majmaah, Saudi Arabia. His research areas include Computer Networks and applications, Network Security, Cyber Security, with specialization in Information Technology. He can be reached at ma.alshehri@mu.edu.sa

Dr. Shaik ShakeelAhamad is currently working as an Assistant Professor in CCIS, Majmaah University, Kingdom of Saudi Arabia. He holds a PhD in Computer Science from the University of Hyderabad and IDRBT (Institute For Development and Research in Banking Technology), Hyderabad, India in the realm of secure mobile payment protocols and formal verification. He has published more than 25 research papers in reputed International journals / Proceedings indexed by ISI, Scopus, ACM Digital Library, DBLP, and IEEE Digital Library. He is serving as a Review Committee Member in many ISI indexed journals. He is CEI (Certified EC Council Instructor), ECSA (EC Council Certified Security Analyst), CHFI (Computer Hacking Forensic Investigator), Certified Threat Intelligence Analyst (CTIA), and Certified Application Security Engineer (CASE) – Java. His research interests include cloud-based mobile commerce, secure mobile healthcare frameworks, Blockchain technology, Application Security, and Smart Grids. He is a member of the IEEE, Association for Computing Machinery (ACM), ISACA, and OWASP (Open Web Application Security Project). He can be reached at ahamadss786@gmail.com&s.ahamad@mu.edu.sa