Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.98549556

COMMUNITY CLOUD BASED SECURE MOBILE GOVERNMENT FRAMEWORK WITH FORENSICS READINESS

Ayoub Saud Ahmad Albader[1] and Shaik Shakeel Ahamad[2]
[1&2]Department of Information Technology, College of Computer and Information Sciences
Majmaah University, Al-Majmaah, 11952, Saudi Arabia
[2]ahamadss786@gmail.com , [2]s.ahamad@mu.edu.sa , [1]431104324@s.mu.edu.sa &
[1]albaderayoub@gmail.com

Abstract— The huge adoption of Mobile Governance services in both the developed and developing countries attracted many cyber criminals. Existing Mobile Governance frameworks are vulnerable at the user level, communication level and cloud level, so cyber criminals exploit many attack surfaces which includes User Credentials, Mobile Application Integrity, Hardware/Device Integrity and communication security. Existing Mobile Government solutions needs to ensure security at rest, during transmission and at the cloud side, in addition to these Mobile Government solutions needs to be ensure forensics readiness. This paper proposes a Community Cloud based Secure Mobile Government (CCSMG) Framework which ensures security at User level, Mobile Application Integrity, Hardware or Device Integrity and communication security, in addition to these our proposed CCSMG framework ensures security at the cloud side and ensures forensics readiness. Proposed protocol has less computational cost and energy cost. CCSMG protocol is verified using Burrows–Abadi–Needham (BAN) logic. CCSMG Framework is threat modeled and implemented successfully.
Keywords—: Community Cloud based Secure Mobile Government (CCSMG); Burrows–Abadi–Needham (BAN); Mobile Government Application (MGA); Forensics Readiness; Mobile Application Integrity; Community Cloud; Communication security; Threat Modeled

Introduction

Huge advancements in the information and communication technologies enabled citizens to get official government services any time anywhere without visiting the offices physically. The usage of smart phones enabled the government to convert from electronic government to mobile government. The main motivation for this research work is according to [8], the cybersecurity market will reach $300 billion by 2027 globally mainly in the realms of network security & privacy, cloud computing and in the telecommunication industry. The most recent DDoS attacks on the Abu Dhabi Commercial Bank and the National Bank of Fujairah brought down their websites [9]. Adoption of cloud computing for mobile government services helped the government in managing the backend services very effectively in terms of efficiency, fast accessing and scalability. Community clouds brings many advantages compared with normal cloud operations, as Community cloud caters the needs of one community such as banking, hospital and government. We define the mobile government as the usage of information and communication technology which includes the Smart phones, Internet, cloud computing, mobile applications, communication devices mobile networks such as 4G and 5G, edge computing and fog computing [2 & 3]. The main objective of mobile government is to bring

convenience to its citizens by enabling government services at their locations [4]. The success and wide adoption of Mobile Government solutions depends on many factors such as citizen's trust, security and privacy of the framework, but the existing solutions does not ensure privacy, security and trust. Government should take the responsibility of citizen's personal and transaction data by adopting secure and reliable mobile government frameworks, these frameworks need to take care of the privacy, security and trust. Existing Mobile Government frameworks are vulnerable at the user level, communication level and cloud level, so cyber criminals exploit many attack surfaces which includes User Credentials, Mobile Application Integrity, Hardware/Device Integrity and communication security. Existing Mobile Government solutions needs to ensure security at rest, during transmission and at the cloud side, in addition to these Mobile Government solutions needs to be ensure forensics readiness which is very important for retrieving evidence from the cloud, network and the devices in case of disputes. The research works presented in [5, 6] is about electronic governance system based on smart cards and digital certificates. The research works presented in [7] is a Multipurpose Electronic Card (MEC) based secure electronic governance system. Organizations needs to have forensics Readiness, so forensics Readiness is defined as "The capability of an organization to collect, preserve, protect and analyze digital evidence so that this evidence can be efficiently used in the court of law" [1].

[10] reviews the efficiency of security policies when addressing threats and vulnerabilities in Saudi Arabia. [11] aims to provide an overview of the extent and success Mobile government in Saudi Arabia. All the solutions in the existing literature [5-7] and [10-11] have the following limitations

i) Key Management is the main hurdle for the acceptance of these solutions
ii) Secrecy of the keys are not possible
iii) No security and privacy in the proposed solutions
iv) There is no forensics readiness
v) Mobile Application Integrity is compromised
vi) Hardware/Device Integrity is compromised
vii) Communication security is compromised
viii) There is no auditing in the existing solutions in the cloud Contributions made

NOTATION	FULL FORM	NOTATION	FULL FORM
MEC	Multipurpose Electronic Card	**TEE**	Trusted Execution Environment
GCC	Government Community Cloud	**TSM**	Trusted Service Manager
SE	Secure Element	**GCA**	Government Certifying Authority
GCCA	Government Community Cloud Application	**TL**	Trust Levels
MGA	Mobile Government Application	**RA**	Registration Authority
CID	Identity of Citizen	**C**	Citizen

ECDSA	Elliptic Curve Digital Signature Algorithm	**IDPS**	Intrusion Detection and Prevention Systems
AES	Advanced Encryption Standard	$\mathbf{LOC_C}$	Location of the Citizen
$\mathbf{SKEY_{GCCC}}$	Shared Symmetric key between 'GCC' & 'C'	$\mathbf{T_C}$	Time Stamp of Citizen
TID	Transaction Identity	$\mathbf{N_C}$	Nonce of Citizen
SERV	Government Service	**TS**	symmetric encryption or decryption function
TH	one-way hash function	**ES**	energy consumed for encrypting or decrypting with AES algorithm
ECPM	Elliptic Curve Point Multiplication	**EH**	energy consumed for hashing with SHA-1 algorithm

a) This paper proposes a Community Cloud based Secure Mobile Government (CCSMG) Framework which ensures security at User level, Mobile Application Integrity, Hardware/Device Integrity and communication security,
b) CCSMG Framework ensures security at the cloud side and ensures forensics readiness.
c) CCSMG Framework has less computational cost and energy cost.
d) CCSMG Framework ensures trust of the citizens
e) CCSMG Framework ensures Auditing in the cloud using cloud forensics tools
f) CCSMG Framework withstands DDoS attacks
g) CCSMG Framework collects evidence from the device, mobile application, Memory Forensics using volatility, Bulk Extractor, SANS, Backlight tools

The rest of the paper is organized as follows. Section 2 proposes a CCSMG framework, Section 3 presents the Threat Modeling of CCSMG framework, Section 4 is about comparison with related works. Section 6 presents the Results and Discussion. Finally, we conclude the paper.

Proposed CCSMG Framework

Central Government (CG), Citizen (C), Government Community Cloud (GCC) and Government Certifying Authority (GCA) are the players of the CCSMG Framework. Central government controls the GCC through dedicated private network. Registration Authority (RA) role is played by the State governments in order to register their citizens.

CCSMG's Framework enhances the trust in the system by using Secure Element (SE), Trusted Execution Environment (TEE), firewalls and Intrusion Detection and Prevention Systems (IDPS) and by installing "Fortguard Anti-DDoS" tool to overcome Denial of Service attacks. CCSMG Framework Employs Auditing Manager (AM) in the GCC which works in coordination with GCA. CCSMG Framework ensures application and communication security will be able to withstand any type of attack. Smart phone of the citizen contains Secure Element, Application Memory, Mobile Government Application in the smart phone and Data Storage at the GCC. GCC has Trusted execution environment (TEE) which is trusted and Applications are isolated and the Keys cannot be compromised. GCC hosts two servers

Authentication Server (AS) and Authorization Server (AuS), AS authenticates the citizens and 'AuS' authorizes services based on the permission and roles. Following are the four locations in which CCSMG framework keeps the data secure

a) **Data in Memory:** The data in the MGA and GCCA needs to be secure and should be able to retrieve the evidence using memory forensics tools.

b) **Data at Rest:** Mobile Government Application (MGA) and GCC Application (GCCA) keeps transaction data secure either temporarily or permanently on the GCC database.

c) **Data in Transit:** Whenever the transaction data of the CCSMG is in transit, the data should not be compromised.

d) **Integrity of the Application:** The integrity of both MGA and GCCA should not be compromised i.e. these applications needs to with stand reverse engineering attacks from intruders.

CCSMG Framework hardens the MGA and GCCA applications by obfuscating, by digitally signing, updating and patching these applications (MGA and GCCA). In addition to these safety measures to these applications adds dynamic library to these applications, this method is called application wrapping.

Our Proposed Protocol: Our proposed protocool has two steps in the protocol,
Step 1: Mobile Government Application authenticates the Citizen (C), after successful authentication 'C' sends {CID, 〖SERV,N〗_C,T_C} to the Government server which is encrypted.

Table 1: NOTATIONS

Step2: GCC→C:{ 〖〖LOC〗_C,TID,SERV,ACK,N〗_G,T_G,CID} 〖SKEY〗_GCCC
Step 2: GCC decrypts and verifies the received message from 'C'
Step2: GCC→C:{ 〖〖LOC〗_C,TID,SERV,ACK,N〗_G,T_G,CID} 〖SKEY〗_GCCC
BAN Logic based Formal Verification of CCSMG Framework
BAN logic [12-14] classifies objects as statements, principals and cryptographic keys. K_GCCC is the shared symmetric key between 'GCC' and 'C'.
Step 2: Citizen 'C' receives { 〖〖LOC〗_C,TID,SERV,ACK,N〗_G,T_G,CID} 〖SKEY〗_GCCC and decrypts the message received from 'G',
C believes G said: { 〖〖LOC〗_C,TID,SERV,ACK,N〗_G,T_G,CID} 〖SKEY〗_GCCC-(1)
C believes # N_G ----(2)
C believes # T_G ---(3)
C believes # LOC--(4)
From the statements (1) to (4) messages communicated among the entities are secure.
Forensics Readiness: Community Cloud based Secure Mobile Government (CCSMG) Framework ensures forensics readiness from the citizen's and community cloud's perspective.

In case of disputes citizens or law enforcement agency can retrieve live evidence from a smart phone or a desktop or laptop using volatility [18] and Belkasoft RAM Capturer tools [19]. UFED cloud analyzer is used to do data and metadata analysis on the collected data and information in the Community Cloud of the government. Diffy [20] provides cloud service and data transparency in the Community Cloud of the government.

THREAT MODELING of CCSMG Framework

In CCSMG framework threat modeling is classified in three steps

(1) Assets and access points identification and the trust levels: An asset is a valuable thing owned by a player of CCSMG framework, and the adversaries wants to manipulate it. Access points are the interfaces through which the adversaries try to can interact with the system in order to gain access to assets. Intruders use access points to enter into the system. There are different levels of trust defined by boundaries.

List of Assets in our proposed CCSMG framework: Mobile Government Application (MGA), Smart Phone, TEE (Trusted Execution Environment) in the GCC side.

List of Access Points (AP) in our proposed CCSMG framework: Mobile Government Application (MGA), Smart Phone.

Trust Levels (TL) in CCSMG framework: There are 3 trust boundaries in CCSMG framework

(1) Citizen and Device boundary: Citizen and Smart phone boundary is between Citizen and the MGA in the SE (Secure Element) of the smartphone.

(2) Recognize and Rank all the possible threats: Threats are recognized by examining the assets and access points in the CCSMG framework which compromise the security properties such as authentication, confidentiality, non-repudiation, availability and integrity.

(3) Discover solutions and make mitigation plan: After recognizing the assets and threats there should be solutions to overcome these threats.

a) Solutions for Spoofing: Spoofing is not possible in CCSMG framework as all the entities store their credentials in the SE and TEE.

b) Solutions for Tampering: Tampering is not possible in CCSMG framework as all the entities exchange only encrypted messages among themselves.

c) Solutions for Repudiation: CCSMG employs Auditing Manager (AM), which works in coordination with GCA.

d) Solutions for Information Disclosure: Information disclosure is not possible in CCSMG framework as all the entities exchange only encrypted messages among themselves which ensures confidentiality.

e) Solutions for Denial of service: CCSMG framework uses “Fortguard Anti-DDoS” tool in order to overcome Denial of Service attacks.

f) Solutions for Elevation of privilege: End to end security which involves application and communication security will be able to overcome attacks in order to elevate the privileges.

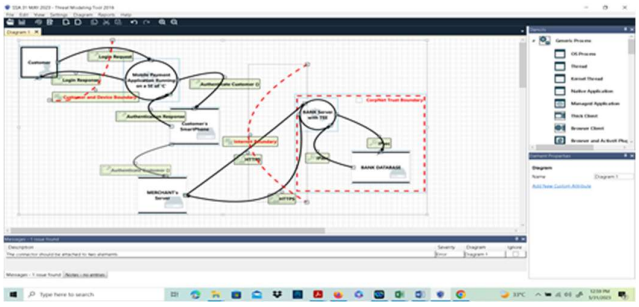

Figure 1: Threat Modeling of CCSMG framework

COMPARISION WITH RELATED WORKS

Research Works Features	[5]	[6]	[7]	Our Proposed CCSMG framework
Confidentiality	No	No	Yes	Yes
Authentication			Yes	Yes
Integrity	No	No	Yes	Yes
Ensures Application Security	No	No	No	Yes
Ensures Communication Security	No	No	Yes	Yes
Withstands Heartbleed Vulnerability	No	No	Yes	Yes
Withstands Replay Attacks	No	No	No	Yes
Withstands Man-In-The-Middle Attacks	No	No	No	Yes
Withstands Impersonation Attacks	No	No	No	Yes
Withstands reverse engineering attacks	No	No	No	Yes
Ensures Auditing in the Cloud	No	No	No	Yes
Trust	No	No	No	Yes

Table 2: Comparison with related works

Results and Discussion

We This section compares CCSMG framework with the related works in terms of computational cost and energy cost. Computational cost is measured in seconds and energy cost is measured in Micro Joules, Table 2 and 3 highlights the comparisons. As per [15] TH=0.0004 and TS=0.1303 calculated in seconds, as per [17] , ES= 1.21 Micro Joules/byte and EH is 0.76 Micro Joules. ECPM is 578.55 Micro Joules [16].

Protocols Features	[5]	[6]	[7]	OUR Proposed CCSMG framework
Computation cost of the Citizen (C) in seconds	2 TS =0.2606 seconds	3TS 0.391	2 TS =0.2606 seconds	1 TS = 0.1303 seconds

Table 3: Computational Cost Comparison of the CCSMG with the related works

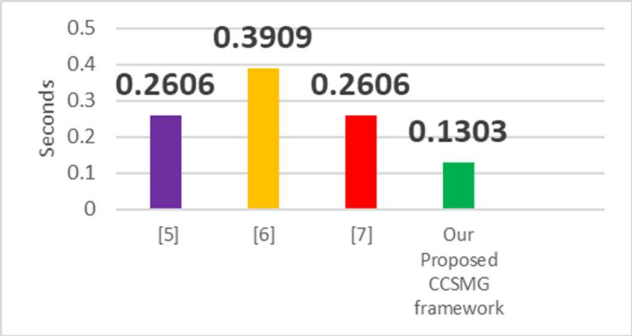

Figure 2: Computational Cost Comparison of the CCSMG with the related works

Protocols Features	**[5]**	**[6]**	**[7]**	**OUR Proposed CCSMG framework**
Energy cost for Citizen (C) in Micro Joules	2ES= 2.42 Micro Joules	3ES= 3.63 Micro Joules	2ES= 2.42 Micro Joules	1ES= 1.21 Micro Joules

Table 4: Energy Cost Comparison of the CCSMG with the related works

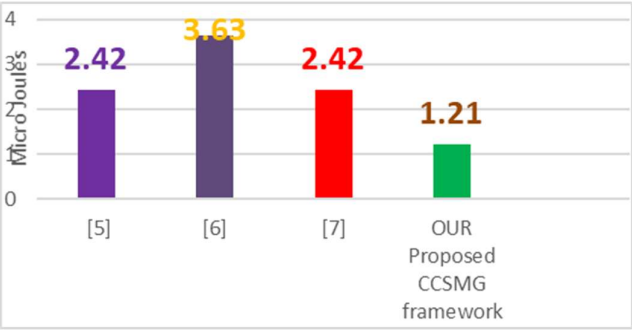

Figure 3: Energy Cost Comparison of the CCSMG with the related works

Conclusion

Mobile Governance services are the main target of many cyber criminals, existing solutions are vulnerable to mobile application, communication level and cloud level attacks. This research work proposes a Community Cloud based Secure Mobile Government (CCSMG) Framework which ensures security at User level, Mobile Application Integrity, Hardware or Device Integrity and communication security, in addition to these our proposed CCSMG framework ensures security at the cloud side and ensures forensics readiness. Proposed protocol has less computational cost and energy cost. CCSMG protocol is verified using Burrows–Abadi–Needham (BAN) logic.

References

https://www.isaca.org/resources/isaca-journal/past-issues/2014/importance-of-forensic-readiness

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

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.

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

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

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

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

https://www.businesswire.com/news/home/20230123005388/en/Cybersecurity-Market---Global-Forecast-to-2027-Opportunities-Emerging-in-Increasing-Use-of-AI-ML-And-Blockchain-Technologies-for-Cyber-Defense---ResearchAndMarkets.com

https://thecyberexpress-com.cdn.ampproject.org/c/s/thecyberexpress.com/cyber-attack-on-uae-banking-sector-adcb-nbf/amp/

Alharbi, A.S., Halikias, G., Rajarajan, M. et al. A review of effectiveness of Saudi E-government data security management. Int. j. inf. tecnol. 13, 573–579 (2021). https://doi.org/10.1007/s41870-021-00611-3

Alharbi, A.S., Halikias, G., Yamin, M. et al. An overview of M-government services in Saudi Arabia. Int. j. inf. tecnol. 12, 1237–1241 (2020). https://doi.org/10.1007/s41870-020-00433-9

S. Muhammad, Z. Furqan, and R. K. Guha, "Understanding the intruder through attacks on cryptographic protocols," in Proc. Annual Southeast Conference, Melbourne, Florida, USA, vol. 2006, pp. 667–672.

M. Abadi, M. Burrows, C. Kaufman, and B. Lampson, "Authentication and delegation with smart-cards," Sci. Comput. Program., vol. 21, no. 2, pp. 93–113, Oct. 1993.

M. Burrows, M. Abadi, and R. Needham, "A logic of Authentication," ACM Trans. Comput. Syst., vol. 8, no. 1, pp. 18–36, Jan. 1990.

Yang, J.-H., Chang, Y.-F., & Chen, Y, "An efficient authenticated encryption scheme based on ecc and its application for electronic payment," Information Technology and Control, vol. 42, no. 4, pp 315–324, 2013.

Maged Hamada Ibrahim, Saru Kumari, Ashok Kumar Das, and Vanga Odelu, "Jamming resistant non-interactive anonymous and unlinkable authentication scheme for mobile satellite networks," Security Comm. Networks, vol. 9, pp 5563–5580, 2017.

Jen-Ho Yang, Ya-Fen Chang, and Yi-Hui Chen, "An Efficient Authenticated Encryption Scheme Based on ECC and its Application for Electronic Payment," Information Technology and Control, vol.42, No.4, 2013.
https://www.volatilityfoundation.org/
https://belkasoft.com/ram-capturer?utm_term=&utm_campaign=Belkasoft+Evidence+Center+X&utm_source=adwords&utm_medium=ppc&hsa_acc=9976381333&hsa_cam=15354488620&hsa_grp=146063170264&hsa_ad=612093065895&hsa_src=g&hsa_tgt=dsa-1748386368887&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_ver=3&gclid=Cj0KCQjwj_ajBhCqARIsAA37s0z70O3GH1mw1USa8e6heWTM88DFFVCeXCO64StyeAOawI2OwM9Di8EaApN4EALw_wcB
https://diffy.website/