Centralized Smart Government Architecture based on Trust Manager

[1]Shaik Shakeel Ahamad
[1]s.ahamad@mu.edu.sa
College of Computer and Information Sciences, Majmaah University, Majmaah 11952, Saudi Arabia

Summary
The rapid growth and development of ICT (Information and Communication Technology) and internet services has boosted the adoption of Mobile Government services all around the globe. There is a huge increase in the adoption of government services during COVID-19 pandemic. Existing Mobile Government (MG) solutions are not trustworthy and secure. This paper provides secure and trustworthy solution for mobile government, proposes a centralized smart governance architecture which is based on trust manager. Our proposed work has Wireless Bridge Certifying Authority (WBCA) and Wireless Public Key Infrastructure (WPKI) thereby ensuring security and privacy. Our proposed work ensures trust with WBCA as WBCA acts as a Trust Manager (TM). Proposed protocol has less computational cost and energy cost

Keywords: *Wireless Bridge Certifying Authority (WBCA), Wireless Public Key Infrastructure (WPKI), Mobile Government (MG), Trust Manager (TM)*

1. Background

The rapid growth and development of ICT (Information and Communication technology) and internet services has boosted the adoption of Mobile Government services all around the globe. There is huge rise in the usage of smart phones for payments, voting and government services [1]. The usage of ICT and internet services played very important role in changing the priorities of government [2]. The unprecedented growth and development of wireless technologies boosted the morale and confidence of citizens in the adopting Mobile Government services [3]. UN defines electronic government as the usage of ICT which includes the Internet, cloud computing, mobile and fog computing [4]. According to [7] Mobile government is defined as an approach and its implementation using wireless networks and smartphones, applications, and communication devices for enhancing the advantages to all the participants in the mobile government which includes citizens, business establishments and all the government entities [7].
[5] defines Mobile Government as an approach which uses wireless technology, cloud and fog computing compared to the conventional e- government solutions [5]. The main aim of mobile government is to deliver services to its citizens at their current locations [6]. The favorable outcome of M-Government solutions depends on citizen's trust, security and privacy of the framework, but the existing solutions are not trustworthy and secure. The main hindrance in the massive growth of Mobile Government include lack of laws, lack of trust, security and privacy. The government should ensure the safety and security of citizen's personal data and the transaction data. The government should guarantee the citizens that their privacy is protected and will overcome all the vulnerabilities in the government applications and in the wireless networks. Most of the works in the literature of mobile government does not focus on trust and security. We are the pioneers in proposing a trustworthy and secure mobile Government framework which ensures trust and security. Authors of [8, 9] has proposed an electronic governance system which is based on smart cards and digital certificates. Authors of [10] has proposed a secure electronic governance system based on Multipurpose Electronic Card (MEC). All the above solutions have the following limitations

i) Management of keys are not possible
ii) Secrecy and newness of the stored keys are not possible
iii) communication and application security are compromised
iv) There are no evidences of security and privacy in the proposed solutions

The following are the contributions made

a) Proposes a centralized smart governance architecture which is based on trust manager.
b) Our proposed work has Wireless Bridge Certifying Authority (WBCA) and Wireless Public Key

Manuscript received December 5, 2021
Manuscript revised December 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.12.78

Infrastructure. Thereby ensuring security and privacy.

c) Our proposed work ensures trust with WBCA as WBCA acts as a Trust Manager (TM).
d) Proposed protocol has less computational cost and energy cost.

The rest of the paper is organized as follows. Section 2 proposes a centralized smart government architecture based on trust manager, Section 3 presents the Security analysis of our proposed system, Section 4 presents the comparative analysis of the protocol with related work. Section 5 presents the comparative analysis of the protocol with related work. Section 6 presents the performance analysis of the protocol with related work. Finally, we conclude the paper with conclusion in section 6.

2. Proposed Centralized Smart Government Architecture based on Trust manager

State Government, Central Government, Citizen, Mobile Government Community Cloud (M-GOVT Community Cloud) and Certifying Authority (CA) are the participants' in the proposed framework. Figure 1 depicts the proposed M-GOVT architecture containing community cloud which is used for only mobile governance needs. Central government controls the M-GOVT community cloud, all the state governments connects with the M-GOVT community cloud through dedicated network. State governments acts as a Registration Authority (RA) and caters the needs of citizens at the local level. Our proposed framework ensures trust as trust plays vital role in the success Mobile Government. Mobile Government's success depends on the collaboration of government institutions such as bank and CA involved in the framework. If all the Mobile Government transactions are transparent and accountable, then it ensures trust in all the citizens. Certifying Authority (CA) is a trust manager in our framework responsible for ensuring trust. CA also issues short lived certificates and X.509 v3 certificates. Our proposed Mobile Government framework uses Wireless Public Key Infrastructures (WPKIs) for all the mobile government services. Wireless Bridge Certification Authority (WBCA) is used to link different state government PKIs. Our proposed framework installs and uses firewalls and Intrusion Detection and Prevention Systems (IDPS) in order to overcome Network security configurations and Internet protocol vulnerabilities.

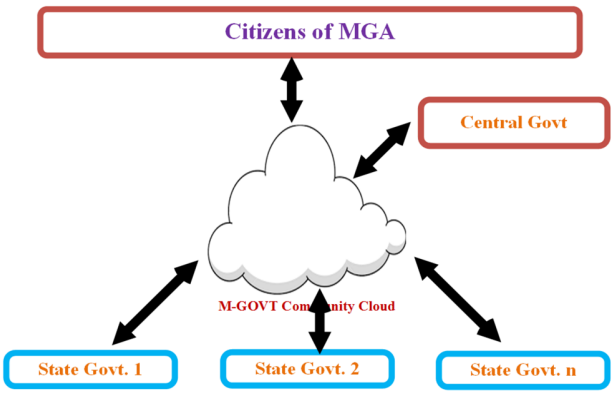

Fig. 1. Proposed M-GOVT architecture

Notation	Full-Form/Meaning
$SKEY_{GC}$	Session Key Shared between the Citizen (C) and Government (G)
CID	Citizen (C)'s Identity
T_C	Citizen (C) generated Time Stamp
T_G	Government (G) generated Time Stamp
N_C	Nonce generated by Citizen (C)
N_G	Nonce generated by Government (G)
ACK	Ack
TID	Transaction ID
SERVICE	Service provided by
AuS	Authorization Server
AS	Authentication Server
C	Citizen
G	Government

TABLE I. NOTATIONS

Technical Architecture: There are two servers at the M-GOVT end, and they are Authentication Server (AS) with credential directory, and Authorization Server (AuS) with identity directory. Authentication Server (AS) verifies the identity of the citizens, when they try to use the government services. Authorization services are delivered to the authorized citizens by the Authorization Server (AuS), these services are delivered based on the role and permissions of the citizens and the government policies which are in force.

Our Proposed Protocol: Our propsed protocool has two steps in the protocol, Figure 2 shows the two steps

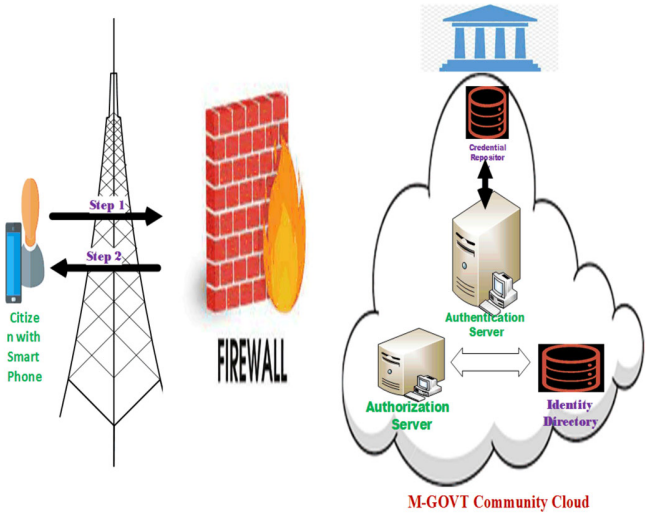

Fig. 2. Proposed Protocol in M-GOVT Framework

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

Step 1: Citizen (C) authenticates himself to the mobile application with a PIN. Citizen sends the encrypted message $\{CID, SERVICE, N_C, T_C\}$to the Governmnet server.

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

Step 2: Government (G) server decrypts the encrypted message using the session key and provides the requested services if the received message is authentic.

3. Security Analysis

Confidentiality: Encrypted messages are encrypted using session keys generated by the mobile government application which ensures confidentiality property.

Integrity: Proposed mobile governance framework adopted application and communication security thereby ensuring integrity property.

Mutual Authentication: Short lived, X.509 certificates and session keys ensure mutual authentication in the proposed mobile governance framework.

Replay Attacks: Encrypted messages are encrypted using session keys generated by the mobile government application. Encrypted messages also contain nonce and timestamps, which helps in withstanding replay attacks.

Impersonation Attacks: Encrypted messages are encrypted using session keys generated by the mobile government application. Encrypted messages also contain nonce and timestamps, which helps in withstanding impersonation attacks.

Man-In-The-Middle Attacks: Encrypted messages are encrypted using session keys generated by the mobile government application. Encrypted messages also contain nonce and timestamps, which helps in withstanding Man-In-The-Middle attacks.

4. Comparative Analysis with Related Work

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

Protocols / Features	[8]	[9]	[10]	OURs
Mutual Authentication	✓	✓	✓	✓
Confidentiality	✓	✓	✓	✓
Authorization	✓	✓	✓	✓
Integrity	✓	×	×	✓
Replay attacks	✓	✓	✓	✓
Impersonation attacks	✓	✓	✓	✓
Man In The Middle Attack	✓	✓	✓	✓
Trust	×	×	×	✓
Privacy	×	×	×	✓

Table 2 brings the comparative analysis of our proposed protocol with the related works [8, 9 & 10]. Our proposed protocol out performs the protocols discussed in the literature.

5. Performance Analysis with Related Work

Table. 3: Computational Costs of the proposed protocol

Protocols Features	[8]	[9]	[10]	OURs
Computation cost of the Citizen (C) in seconds	2 TS =0.2606 seconds	3TS =0.3909	2 TS =0.2606 seconds	1 TS = 0.1303 seconds
Computation cost of the Mobile Government (MG) in seconds	2 TS =0.2606 seconds	3TS =0.3909 seconds	2 TS =0.2606 seconds	1 TS = 0.1303 seconds

Table 3 presents the comparative analysis of the computational cost of the proposed protocol against the protocols discussed in the related works. The notations used in the table are TH and TS, denoting the complexity of time for computing the one-way hash function (TH) and symmetric encryption/decryption (TS) operation. As shown in [13], the time complexities are TH = 0.0004 and TS = 0.1303 in seconds. One ECPM (Elliptic Curve Point Multiplication) is equal to 0.001015 seconds from [14]. Clearly, our proposed protocol has better performance and is shown in Figure 3.

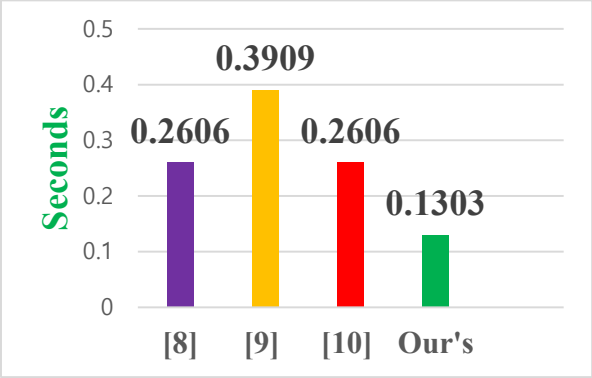

Fig. 3. Computational Cost Comparison

Table 4 presents the energy consumption of our proposed protocol against the protocols discussed in the related works. As shown in [15], the energy consumed to generate encryption/decryption using the AES algorithm is (ES): 1.21 Micro Joules/byte and to calculate SHA-1 hash (EH) is 0.76 Micro Joules. The energy consumption of One ECPM (Elliptic Curve Point Multiplication) is equal to 578.55 Micro Joules from [14]. As shown in the table, our proposed protocol outperforms other works based on the same platform and is shown in Figure 4.

Table. 4: Energy Costs for the proposed protocol

Protocols Features	[8]	[9]	[10]	OURs
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
Energy cost for Mobile Government (MG) in Micro Joules	2ES= 2.42 Micro Joules	3ES= 3.63 Micro Joules	2ES= 2.42 Micro Joules	1ES= 1.21 Micro Joules

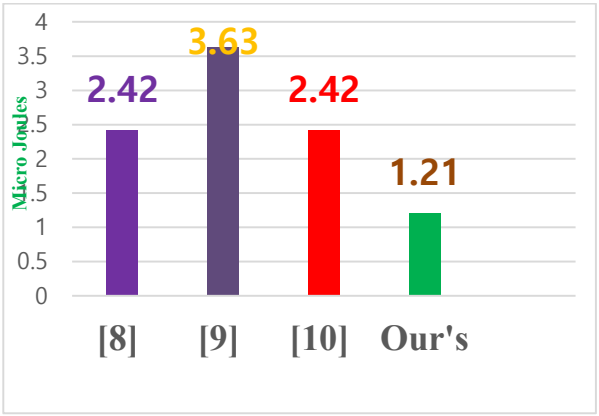

Fig. 4. Energy Cost Comparison

6. Conclusion

This paper proposes a centralized smart governance architecture which is based on trust manager. Our proposed work has Wireless Bridge Certifying Authority (WBCA) and Wireless Public Key Infrastructure (WPKI) thereby ensuring security and privacy. Our proposed work ensures trust with WBCA as WBCA acts as a Trust Manager (TM). Proposed protocol has less computational cost and energy cost. Our proposed framework overcomes the flaws in the existing literature.

Acknowledgments

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.

[13] 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.

[14] 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.

[15] 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.

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