© 2019 IJSRST | Volume 6 | Issue 6 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology
DOI : https://doi.org/10.32628/IJSRST196642

Implementation for Quick Response Code

K. Ravikumar, R. Geetha
Assistant Professor, Department of Computer Science, Tamil University, Thanjavur, Tamil Nadu, India

ABSTRACT

Quick Response (QR) codes are versatile. a chunk of long trilingual text, a connected URL, an automatic SMS message, an identity card or simply regarding any data is embedded into the two-dimensional barcode. as well as moderate equipped mobile devices, QR Codes will connect the users to the data quickly and simply. The operations to retrieve or store QR codes are unbelievably easy and fast, and with mobile devices, build them the best academic tools for teaching and learning. QR codes are all over and most of the people have mobile phones equipped with QR code readers. though QR codes existed for over fifteen years, there aren't such a lot of analysis applications during this space.

Keywords : Quick Response, Cyber-Physical Networked Systems, MAC, PCREF, Key Generation Center, Send Data Storing Center

I. INTRODUCTION

In Cyber-Physical Networked Systems (CPNS), the competitor will inject false measurements into the controller through compromised sensing element nodes, that not solely threaten the safety of the system, however additionally consume network resources. To manage this issue, variety of En-route filtering schemes are designed for wireless detector networks. En-route filtering may be a theme by which intermediate nodes make sure the genuineness of messages and filter them once those messages travel through the network. during this existing En-route filtering schemes are supported authentication. once a report is transmitted from a detector node to the controller, every forwarding node checks whether the forwarding reports really carry valid MACs.

In the proposed system we implement a novel En-route filtering scheme against false data injection attacks in cyber-physical networked systems. When a report is transmitted from a sensor node to the controller, each forwarding node checks whether the forwarding reports actually carry valid MACs. If not, the report is considered afalse one forged by the adversary and then dropped. Otherwise, the report is forwarded to the next forwarding nodes.

In Cyber-Physical Networked Systems (CPNS), the competitor will inject false measurements into the controller through compromised detector nodes, that not solely threaten the safety of the system, however additionally consume network resources. To take care of this issue, variety of En-route filtering schemes are designed for wireless detector networks. However, these schemes either lack resilience to the quantity of compromised nodes or depend upon the statically designed routes and node localization, that aren't appropriate for CPNS. during this paper, we tend to propose a Polynomial-based Compromise-Resilient En-route Filtering theme (PCREF), which might filter false injected information effectively and succeed a high resilience to the quantity of compromised nodes

while not counting on static routes and node localization.

PCREF adopts polynomials rather than Message Authentication Codes (MACs) for endorsing measure reports to attain resilience to attacks. every node stores two sorts of polynomials: authentication polynomial and check polynomial, derived from the primitive polynomial, and used for endorsing and validating the activity reports. Through in depth theoretical analysis and experiments, our information shows that PCREF achieves higher filtering capability and resilience to the big range of compromised nodes as compared to the present schemes. IN Cyber-Physical Networked Systems (CPNS), the competitor will inject false measurements into the controller through compromised detector nodes, that not only threaten the protection of the system, however additionally consume network resources.

Data Owner

- Login
- Key Generation Center (KGC)
- Data owner (set Access Policy, Encrypt File)
- Send Data Storing Center

Data Storing Center

- Store Data

User

- Authentication (Registration /Login)
- User Access
- View Available Files
- User Get File
- Decrypt File

II. METHODS AND MATERIAL

MODULES CLARIFICATION

Data Client

Login

In Login type module presents user, a type with username and form fields. If the user enters a valid username/password combination they're going to be granted to access information. If the user enters invalid username and password that user will be considered as unauthorized user and denied access a valid user.

Authentication Polynomial

It's a key authority that generates public and secret parameters for CPABE. it's to blame of issue, revoking, and in charge attribute keys for users. It grants differential access rights to individual users supported their attributes. Key generation is that the method of generating keys for cryptography. A key's used to encrypt and decrypt no matter whatever is being encrypted/decrypted.

Data owner (set Access Policy code, encode File Access code)

It's a consumer who owns information, and needs to transfer it into the external information storing center for simple sharing or for price saving. an information owner is accountable for process (attribute based) access policy, and implementing it on its own information by encrypting the information under the policy before distributing it. information Owner to induce key from key generator encode the file.

encryption is that the conversion of information into a kind, known as a cipher text that can't be simply understood by unauthorized folks.

Message Authentication Code

Data storing center store the data Dataowner Encrypt the file and Store Data storing center.

Data Storing Center

It's an entity that has an information sharing service. it's responsible of controlling the accesses from outside users to the storing information and providing corresponding contents services. the information storing center is another key authority that generates customized user key with the KGC, and problems and revokes attribute cluster keys to valid users per every attribute, that are used to enforce a fine-grained user access management. information storing center store the information. the data Storage Centers provides offsite record and tape storage, retrieval, delivery and destruction services.

III. RESULTS AND DISCUSSION

User Authentication (Registration /Login)

New user access information storing means that should, new User will enter our details and register here. In Login form module presents users, a form with username and password fields. If the user enters a valid username/password combination they'll be granted to access information. If the user enters invalid username and password that user is going to be thought-about as unauthorized user and denied access to it user.

User Access Code

In this module the user to check our attributes and access policy.

View Available Files

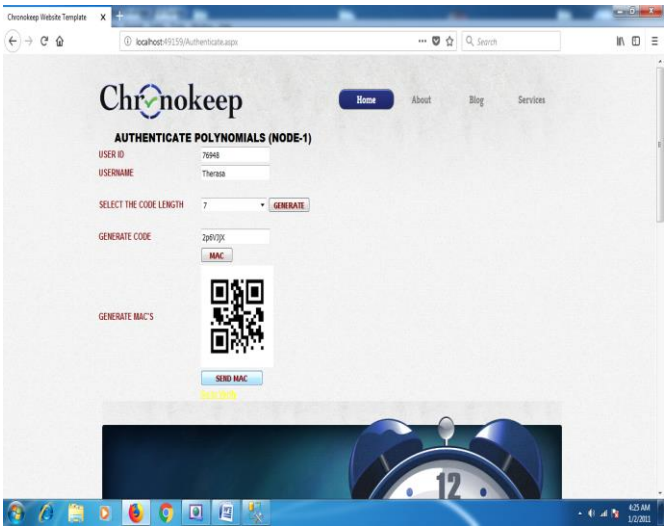
Data Storing Center Store the number of files that files are displayed authorized user based on user access policy.

User Get File Access code

It's an entity who needs to access the information. If a user possesses a group of attributes satisfying the access policy of the encrypted information, and isn't revoked in any of the valid attribute teams, then he will be able to decode the cipher text and acquire the information User to select specific file and acquire Key from Key Generation Center.

Decrypt File Access Code

Decoding is that the reverse method to encoding. Frequently, identical Cipher is used for each encryption and decryption. Whereas encryption creates a Cipher text from a Plaintext, encoding creates a Plaintext from a Cipher text. User uses that specific file key decodes and save that file.



IV. CONCLUSION

To achieves safer and fine-grained information access management within the information sharing system. we tend to demonstrated that the planned theme is economical and scalable to firmly manage user information within the information sharing system.

information privacy and confidentiality within the information sharing system against any system managers still as adversarial outsiders while not corresponding (enough) credentials. The advantage CP-ABE comes solve key escrow problem. Secure two-party computation between the key generation center and also the information storing center information privacy and confidentiality within the information sharing system against any system managers yet as adversarial outsiders while not corresponding (enough) credentials. Selective attribute key distribution on high of the ABE.Secure and fine-grained information access management within the information sharing system.

V. REFERENCES

[1]. A. Lewko, A. Sahai, B. Waters , "Revocation Systems with Very Small Private Keys" ,Proc. IEEE Symposium on Security and Privacy 2010, pp. 273–285, 2017.

[2]. A. Boldyreva, V. Goyal, V. Kumar, "Identity-Based Encryption with Efficient Revocation" , Proc. ACM Conference on Computer and Communications Security 2008, pp. 417–426, 2017

[3]. L. Cheung, C. Newport, "Provably Secure Ciphertext Policy ABE" ,ACM Conference on Computer and Communications Security, pp. 456–465, 2017.

[4]. L.Ibraimi, M. Petkovic, S. Nikova, P. Hartel, W. Jonker, "Mediated Ciphertext- Policy Attribute-Based Encryption and Its Application" , Proc. WISA 2009, LNCS 5932, pp. 309–323, 2016.

[5]. S. Yu, C. Wang, K. Ren, W. Lou, "Attribute Based Data Sharing with Attribute Revocation", Proc. ASIACCS '10, 2015.

[6]. Suppat Rungraungsilp, Mahasak Ketcham, Virutt Kosolvijak, and Sartid Vongpradhip, "Data hiding method for QR code based on watermark by compare DCT with DFT domain‖", International Conference on Computer and Communication Technologies (ICCCT'2012), May 26-27, 2012.

[7]. Kuan-Chieh Liao, "A novel user authentication scheme based on QR-code", Journal of networks, vol. 5, no. 8, August 2010.

Cite this article as :

K. Ravikumar, R. Geetha, "Implementation for Quick Response Code", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 6 Issue 6, pp. 249-252, November-December 2019. Available at doi :
https://doi.org/10.32628/IJSRST196642
Journal URL : http://ijsrst.com/IJSRST196642