VOL 4 (2020) NO 3

e-ISSN : 2549-9904
ISSN : 2549-9610

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

Security Architecture for Low Resource Devices in Smart City using Cloud

Muneer Ahmad Dar[#]

[#] *National Institute of Electronics and Information Technology (NIELIT), SIDCO Electronics Complex Rangreth, Srinagar J&K , INDIA*
E-mail: muneerdar07@gmail.com

***Abstract*— The world is moving towards modernization with the help of smart devices used in smart cities to make the whole lot intelligent and smart. These smart devices are extensively used in smart city and are capable of doing everything which one can do with the normal desktop computer. These smart devices like Smartphone have computational limitations are not able to store a large data to be used and collected in a smart city. In this paper, we propose a novel security architecture which first uses the Elliptic Curve Diffie Helman Key Exchange Algorithms to exchange the keys between the two low power devices (Smartphone). The keys are used to encrypt the large data (images and videos etc). The data is encrypted using the private keys of a device and then send to the cloud for safe storage. The data can be only accessed by the communicating device with the same key. The proposed security architecture enables these smart devices to store the huge data collected from the smart city to store on the cloud. If another device requests the same set of data, the keys can be shared secretly and the communicating device can be allowed to download the data directly from the cloud. This architecture relieves the Smartphone from the storage limitation and also enables it to communicate with faster speed and securely.**

***Keywords*— smartphone; elliptic curve; smart city; cloud.**

I. INTRODUCTION

The idea behind the implementation of smart city is to make use of intelligent devices so as to control everything smartly. One of the prominent smart devices is a smart phone capable of doing every job as can be done with the desktop computer. The smart phone is carried by almost every citizen with the intension to always be connected and ease the life. The prominent Smartphone operating systems – Android and IOS are numerously used by the users [9]. The only drawback of using these devices is the limited capability to store the data and computationally less power full as compared to desktop computers [2]. In smart city there are numerous challenges that a citizen can face in terms of privacy and security [10] of the sensitive data stored in their personal hand held devices. The users in a smart city are accessing their bank accounts through their smart phones and storing every critical information in there devices [11]. The smart devices are not able to store huge data in there devices and at the same time are not able to use the traditional algorithms to encrypt and decrypt the data.

Without precedent for the historical backdrop of mankind, more them half of the populace is presently living in large urban communities. This situation has raised concerns related frameworks that give fundamental administrations to residents. While developing the solutions for its users in a smart city, huge amount of data is collected and the possibility of data breach is evident in such scenarios. The Figure 1 provides general over view of a smart city with capabilities to have smart energy, smart education, smart logistics and many more features.

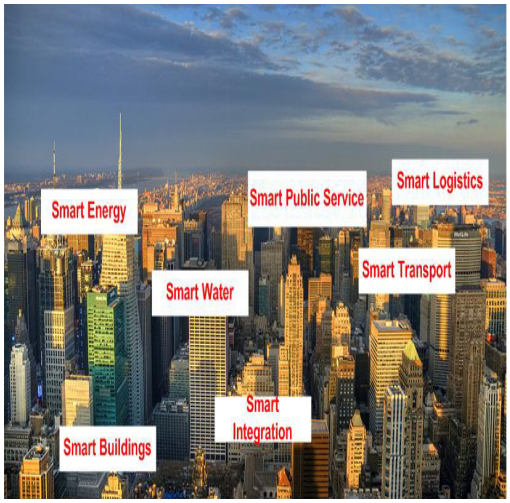

Fig 1: Smart City

The paper is organized as – Section II provides a detailed work done in the area of privacy and security of users in a smart city. The use of cloud by some researchers is also discussed in this section. Section III proposes novel security architecture for the smart devices connected in a smart city. The algorithms that can be implemented to store the data on a cloud and establishment of secure key between the two connecting devices is discussed in this section. In section IV the results are presented and a final conclusion is discussed.

II. Related Work

In this section, we discuss the related research done in the area of resource constrained devices used in a smart city. There are active and passive ways of dealing with the defenses against the various threats and attacks by the intruders, Researchers mainly focused on the passive ways of security [5]. In a classical smart city, the issues related to defenses against the malicious applications have various characteristics, including security service, how data is organized, authorization and management of keys. The various solutions proposed for the security of users in a smart city are mainly of distributed in nature and are obtained from the distributed systems [6]. One of such techniques is a smart grid technique [7]. The methods defined in [6][7] are not enough for securing the users in a smart city particularly for the use of low resource device like a Smartphone. The main reason for the scarcity of the security protocols is the lack of resources of a smart device used in a smart city [8]. The protection of users from over collection of data within a smart city is discussed in [1]. Their [1] research mainly focused on putting the users data on the cloud and did not came up with a solution to ease the pressure from these low power devices to execute an algorithm that is feasible for them. The lightweight session key establishment for android platform using ECC was elaborated [2] and a more robust and computationally feasible approach was implemented.

The Security and protection based on cloud in smart cities is talked about in [18]. Different partners are distinguished and a system for start to finish security/protection highlights for trustable information obtaining, scattering and administration arrangement is created. A different approach is introduced in [19] where the appearance of secure equipment in individual IT gadgets propels provisioning of information security at the edges of the web by means of individual information servers running on advanced mobile phones set-top boxes, secure compact tokens and so forth. A five dimensional model of residents' security in smart urban areas is introduced in [20]. These are: character protection, query security, identity security and area security, impression protection and proprietor protection. The researchers in this paper show how existing security improving innovations can be utilized to save residents' protection.

III. Proposed Security Architecture

The data to be stored on the cloud must be encrypted by the device and then it can be loaded on the cloud for the safe storage. The following architecture depicted in figure 2 is proposed. The smart devices must be able to communicate in a secure way. The Elliptic Curve Key exchange is proposed which is computationally feasible for low power devices [2]. After exchanging the keys, the data is encrypted and the data which includes videos, files and any other confidential data can be stored on the cloud. The data cannot be understood by the intruder and it can be put in a safe custody. If a second device within a smart city wants to access the same data then the keys already exchanged can be used to decrypt the data and safely download it from the cloud.

The proposed architecture addresses the three principle security issues- Privacy, Integrity and Availability.

i. Privacy. The security idea is legitimately related with the demonstration of just permit the right substance, with the right consent, to approach particular information. It can likewise be viewed as the upkeep of a mystery in a message, or information, trade from DEVICE_1 to DEVICE_2. The proposed architecture generates a shared key by making use of Elliptic Cure Cryptography- which is computationally feasible for the smart devices used in a smart city.

ii. Integrity. The integrity of the confidential data is maintained by keeping the data in encrypted form within the cloud. This architecture does not allow the changes in the data and only the authorized devices are allowed to do so.

iii. Availability. Another key issue addressed by our proposed system is that the resources are available to the authorized users without any obstacle. If any other smart device wants to access the resource from within a smart city, the device can get the shared keys from the other device and can directly download the required data from the cloud.

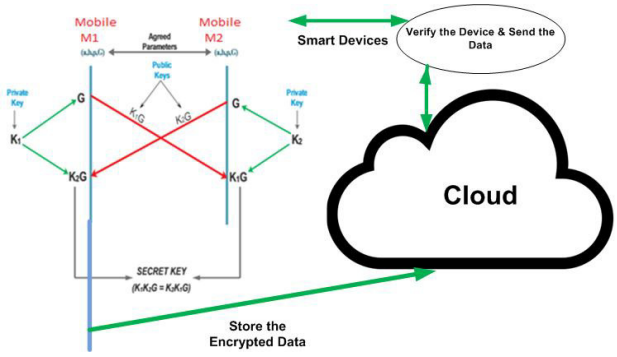

Fig 2. Proposed Architecture

The algorithm 1 below provides the steps to securely store the data on the cloud. The data if needed by any other device must be authenticated and the key must be shared with the communicating device.

Algorithm 1: Secure_Storage (Device_ID, Data)

{

1. Compare the type of the request- to store the data or retrieve the data. Get the result RW;
2. if RW == write then
3. Store the ID of the device along with the encrypted Data
4. else
5. verify the device ID
6. read the encrypted Data
7. return Data
8. end if

}

The traditional Cryptographic algorithms are computationally very expensive when implemented on the low power devices. If we use a key length of 1024 in RSA, same security can be provided by the ECC with a key length of 160 [2].

The parameters used in elliptic curve are a sextuple:

$$T = (P, a, b, G, n, h)$$

The elliptic curve is defined by an equation of the form

$$Y^2 = X^3 + AX + B$$

The detailed description of elliptic curve functionalities for the low power devices is described in one of our paper [2].

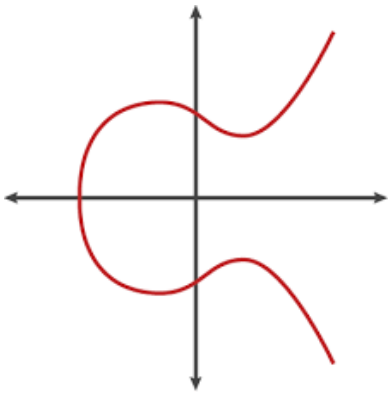

Fig 3. Elliptic Curve

The algorithm 2 provides a sequence of steps to generate the shared keys by the two communicating devices in a smart city.

Algorithm 2: Secure_Key_Exchange (Pub_a, Pub_b)

{

1. DEVICE_1 chooses a random number Na such that Na < N where N is a prime field. This is Na's Private Key
2. DEVICE_1 calculates the public key as Pub_a = Na * G [G is the generator point]
3. DEVICE_1 generates the secret key as S_Key = Na * Pub_b [Pub_b is public key of DEVICE_2]
4. The secret key shared is
5. S_Key = Na * Pub_b = Na * (Nb * G) as Pub_b = Nb * G as generated by DEVICE_2
6. Return S_Key [Na *Pub_b = Nb * Pub_a]

}

Fig 4. ECC Implementation on Android

The two devices only disclose their public keys and the shared key is calculated. The same shared key is used by the devices to encrypt and decrypt the data.

IV. Results and Conclusion

In this research, a novel approach to enhance the capabilities of resource constrained devices is discussed. The proposed architecture is implemented with the android based smart phones and the shared keys are communicated in a open channel. The screen shot of one of the Android based smart phone is presented in figure 4. The smart city model is taken into consideration where millions of users are using their hand-held devices to do lot of intelligent computing and their security concerns are discussed in this paper. As these devices are computationally incompetent to execute algorithms link RSA, DES etc, an Elliptic Curve Cryptography is introduced which is as secure as RSA but at the same time does not take that much of computational overhead as RSA does.

References

[1] Y. Li, W. Dai, Z. Ming and M. Qiu, "Privacy Protection for Preventing Data Over-Collection in Smart City," in IEEE Transactions on Computers, vol. 65, no. 5, pp. 1339-1350, 1 May 2016, doi: 10.1109/TC.2015.2470247.

[2] Dar, Muneer & Khan, Ummer & Bukhari, Syed. (2019). Lightweight Session Key Establishment for Android Platform Using ECC. 10.1007/978-981-13-3122-0_33.

[3] M. A. Dar and J. Parvez, "Security Enhancement in Android using Ellipic Curve Cryptography," Int. J. Secur. its Appl., vol. 11, no. 6, pp. 27–34, 2017.

[4] H. Zhu, R. Lu, C. Huang, L. Chen and H. Li, "An Efficient Privacy-Preserving Location-Based Services Query Scheme in Outsourced Cloud," in IEEE Transactions on Vehicular Technology, vol. 65, no. 9, pp. 7729-7739, Sept. 2016, doi: 10.1109/TVT.2015.2499791.

[5] M. Qiu, W. Gao, M. Chen, J.-W. Niu, and L. Zhang, "Energy efficient security algorithm for power grid wide area monitoring system," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 715–723, Dec. 2011.

[6] J. Blom, D. Viswanathan, M. Spasojevic, J. Go, K. Acharya, and R. Ahonius, "Fear and the city: Role of mobile services in harnessing safety and security in urban use contexts," in Proc. SIGCHI Conf. Human Factors Comput. Syst., 2010, pp. 1841–1850.

[7] A. Paverd, A. Martin, and I. Brown, "Security and privacy in smart grid demand response systems," in Proc. 2nd Int. Workshop Smart Grid Security, 2014, pp. 1–15.

[8] D. Damopoulos, G. Kambourakis,M. Anagnostopoulos, S. Gritzalis, and J. Park, "User privacy and modern mobile services: Are they on the same path?" Personal Ubiquitous Comput., vol. 17, no. 7, pp. 1437–1448, 2013.

[9] M. A. Dar, S. Nisar Bukhari and U. I. Khan, "Evaluation of Security and Privacy of Smartphone Users," 2018 Fourth International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Chennai, 2018, pp. 1-4, doi: 10.1109/AEEICB.2018.8480914.

[10] M. A. Dar and J. Parvez, "Smartphone operating systems: Evaluation & enhancements," 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Kanyakumari, 2014, pp. 734-738, doi: 10.1109/ICCICCT.2014.6993056.

[11] M. A. Dar and J. Parvez, "Enhancing security of Android & IOS by implementing need-based security (NBS)," 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT), Kanyakumari, 2014, pp. 728-733, doi: 10.1109/ICCICCT.2014.6993055.

[12] U. Iqbal, M. A. Dar and S. Nisar Bukhari, "Intelligent Hospitals based on IOT," 2018 Fourth International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Chennai, 2018, pp. 1-3, doi: 10.1109/AEEICB.2018.8480947.

[13] M. A. Dar, "A novel approach to restrict the access of malicious applications in android," 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, 2017, pp. 1-4, doi: 10.1109/ICIIECS.2017.8275927.

[14] V. Dattana, K. Gupta and A. Kush, "A Probability based Model for Big Data Security in Smart City," 2019 4th MEC International Conference on Big Data and Smart City (ICBDSC), Muscat, Oman, 2019, pp. 1-6, doi: 10.1109/ICBDSC.2019.8645607.

[15] R. Srinivasan, A. Mohan and P. Srinivasan, "Privacy conscious architecture for improving emergency response in smart cities," 2016 Smart City Security and Privacy Workshop (SCSP-W), Vienna, 2016, pp. 1-5, doi: 10.1109/SCSPW.2016.7509559.

[16] S. Ghosh, "Smart homes: Architectural and engineering design imperatives for smart city building codes," 2018 Technologies for Smart-City Energy Security and Power (ICSESP), Bhubaneswar, 2018, pp. 1-4, doi: 10.1109/ICSESP.2018.8376676.

[17] F. S. Ferraz and C. A. G. Ferraz, "Smart City Security Issues: Depicting Information Security Issues in the Role of an Urban Environment," 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, London, 2014, pp. 842-847, doi: 10.1109/UCC.2014.137.

[18] Towards Cloud based Smart Cities Data Security and Privacy Management , IEEE/ACM 7th International Conference on Utility and Cloud Computing, 2014

[19] Anciaux, Nicolas & Bonnet, Philippe & Bouganim, Luc & Nguyen, Benjamin & Popa, iulian & Pucheral, Philippe. (2013). Trusted Cells: A Sea Change for Personal Data Services.

[20] A. Martinez-Balleste, P. A. Perez-martinez and A. Solanas, "The pursuit of citizens' privacy: a privacy-aware smart city is possible," in IEEE Communications Magazine, vol. 51, no. 6, pp. 136-141, June 2013, doi: 10.1109/MCOM.20