Smart Contract-Based Alert System for Reduction of Information Privacy Paradox and Fatigue in IoT

Kardan Journal of Engineering and Technology
1 (1) 37–47

Kardan Publications
Kabul, Afghanistan
DOI: 10.31841/KJET.2021.4
https://kardan.edu.af/Research/Kardan_journal_of_engineering_and_technology.aspx#

Riaz Ahmad Ziar
Syed Irfan Ullah
Rafiulllah Omar

Abstract

The introduction of smart devices and the IOT network has led to the creation of large amounts of data that require protection from intrusion. Most users desire to have personal data kept confidential while seeking for platforms that would prohibit their vendors from distributing it to third parties without their consent. However, the users that are conscious of data privacy often share information with third parties, contradicting their intentions in keeping their information confidential. The difference between user intentions and actions regarding data privacy is called privacy paradox while privacy fatigue refers to the weariness of people on implementing security and privacy solutions. In this proposed system we design and develop smart contracts to provide interaction for the IoT device and company which require personal data. A company or Application requests personal information from the device to share the device sends, that information to the smart contract, smart contract uses dynamic rules to check PII in the users' personal information. Base on the PII (,) system would alert users on the limit and risk of sharing personal information through a public network. We used solidity programing language for the modeled of the smart contract. The performance of the contract is evaluated on the Repsten test network.

Keywords: *Smart Contract, Privacy Paradox, Solutions to IoT Privacy Challenges, Privacy Fatigue, Blockchain, Ethereum*

Mr. Riaz Ahmad Ziar, *Lecturer at Faculty of Engineering and Technology, Kardan University, Kabul, Afghanistan and pursuing Master's in Computer Sciences at Abasyn University, Peshawar, Pakistan.*
Dr. Syed Irfan Ullah, *Assistant Professor at Department of Computing, Abasyn University, Peshawar, Pakistan.*
Mr. Rafiullah Omar, *Assistant Professor at Faculty of Computer Science, Salam university, Kabul, Afghanistan.*

Introduction

Technology is one of the primary drivers of businesses as most organizations consider data as one of the valuable assets that helps them to gain competitive advantage. Companies collect data from different sources, such as online stores, search engine reports, and websites, to help them analyze the behavior of customers while creating effective decisions to increase their sales. People have implemented various technologies in their homes to allow them communicate faster and efficiently with others from remote regions. The Internet of things (IoT) is a technology that has helped business and families to share information between multiple smart objects. However, the introduction of IoT has exposed the information privacy of users to a plethora of risks that include loss of data [1]. Information privacy paradox is one of the causes of the security issues where online users share personal data regardless of their data privacy concerns [1]. Information privacy fatigue and paradox are the primary causes of losing privacy in online communication, which relevant organizations should address by providing effective measures, such as user awareness and privacy policies.

2 Literature Review

2.1 Privacy Paradox

According to [1], privacy paradox refers to an online behavior that involves a disclosure of personal information by a user who cares about the privacy of his or her data. A research conducted by Pew Research Center in 2013 reveals that about 86% of the interviewed online users have concerns about information privacy and take multiple measures to enhance confidentiality of their information [4]. Some of the primary techniques that online users implement to protect their information from intruders include, clearing cookies from browsers after accessing emails and other websites [4]. A research by authors of [5] found that users value their browsing history at 7 Euros where anyone would obtain personally identifiable information (PII) of a specific user. The issue of privacy seems to be becoming an outdated concept as most people have become sensitive of the publicly available information, making them to share PII regardless of their privacy attitudes. The researchers suggest the implementation of a lightweight ring structure in IOT components which involves digital signatures to ensure they users stay anonymous [12], [13].

The researchers in [11] support that the cases where developers and engineers of IOT products have been compelled to make simpler privacy policies have yielded more data privacy levels. A study by Beresford. The researchers in [14, 15] provide a solution that utilizes a block chain's smart

contracts to enforce information privacy in networks. in [6] was aimed at investigating the concept of information privacy paradox by determining the willingness of people to buy from two similar stores. The authors had one of the stores sell products at a discount of 1 Euro but require people share their PII while the other did not offer discounts and maintained the privacy of its customers' data. The researchers found out that more people were willing to purchase products at cheaper prices regardless of the data privacy threats [6]. Other sectors with significant privacy paradox issues is the mobile application uses where consumers in the U.S. and China were observed to be willing to continue using a specific mobile app despite the risk of exposure of PII [3]. Therefore, privacy paradox is a primary challenge in enhancing information security in IoT technology and other online applications.

2.2 Privacy Fatigue

In [9], privacy fatigue refers to the state of weariness where users of multiple technological solutions become desensitized due to multiple security and privacy controls given to them. The introduction of measures to reduce cybercrimes, such as antimalware and passwords policies, made people to believe that their data would be kept confidential and private. However, the measures have become a burden to online users because multiple attacks continue to occur, making them to reach a saturation point with the solution and developing a sense of hopelessness [9]. According to [10], people become tiered of the procedures that security organizations offers them as measure to maintain the privacy of their information because it prevents them from performing primary tasks through the IoT technology. For instance, some users claim that it is difficult to stay vigilant all the time when providing personal information as multiple techniques may be used to extract one's PII from other sources [10], [9]. The feelings of tiredness with privacy controls lead to loss of data confidentiality and privacy.

2.3 Contributory Factors

Education levels and experience of users influence their willingness to share personal information through online platforms. According to [7], people with doctoral degrees are the least likely to share personal data while the high school students have the highest probability of sharing PII. The study by [2] support the findings by describing that high school students often join social media sites with the intention of connecting with their friends and later get surprised when they realize the society can access their journals. Besides, users with high levels of education apply stronger security controls in their online platforms to ensure information privacy [2, 7].

System configurations and privacy policies make users to disclose personal data that would lead to privacy paradox. Studies have found that most users that are eager to use the services of a specific application, such smart wearables and social media platforms, often check the box and agree to privacy policies without reading them [1, 8]. Moreover, system and software engineers develop their products with obfuscated policies that make it difficult for users to recognize critical aspects of the information required from them [1]. Most people bypass the documentations in IoT devices while others continue with default security settings, making them lose data privacy.

Social norms influence privacy paradox by making people align their privacy behaviors to things that the society considers as normal. Authors of [1] argue that some software applications, such as Signal, have failed to gain a significant market share due to their intensive privacy configurations that make people prefer alternatives with less privacy and more market share. For instance, one would be willing to use a social media platform that most of his or her friends are using regardless of the high risk of exposing personal data [1]. Therefore, users often align their behavior to contemporaries when using IoT technology with a specific perception by the society.

3 Research Gap

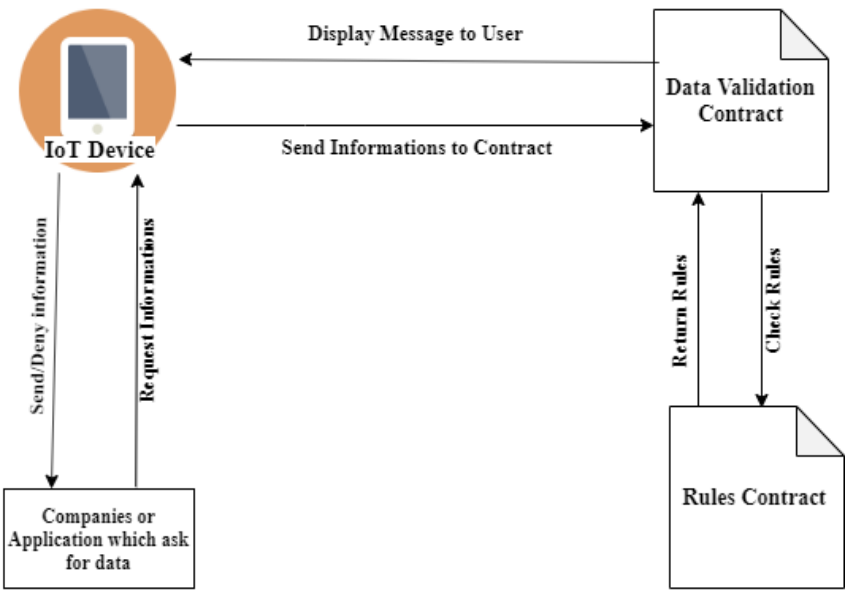
Most of the studies conducted by various researchers serve as an inspiration to analyze the nature of privacy paradox and fatigue while developing practical solutions. Moreover, the findings in the available literature are based on political and emotional opinions based, on the beliefs and ethics underlying the normal behavior of a democratic society. For instance, one may develop a solution to privacy paradox that allows companies, such as Facebook, to collect user information after receiving their consent in a visible way. Designers of IoT systems may use an enhanced user interface that alerts people of various risk actions that might want to take without limiting them of the functionality of a specific node. Therefore, various stakeholders have understudied the possibility of using technological methods, such as advanced user interface, to reduce the gaps between privacy intentions and behaviors.

Most studies indicate that people perform activities that may differ from their intentions without studying the primary cause of the privacy paradox. For instance, studies that have provided education and social norms as contributing factors may have failed to determine the motivation of users in allowing their data to be accessed without gaining anything. For

example, authors in [6] show that people are willing to provide PII if they receive a monetary value without explaining the reason for those who share their data without receiving any money. Therefore, studies that would aim at redesigning the architecture of the IoT systems and other platforms may help reduce privacy paradox and enhance the confidentiality of information.

4 Architecture of the Proposed Solution

Figure 1: Proposed System Architecture



Source: Author's Compilation

1. IoT devices: this represents any device which is connected with the IoT and transfer information
2. Companies or applications: this element of the model represents each company and application that requires information from the devices to be shred.
3. Data validation smart contract: this contract is created to check user data for the personally identified information (PII)(.) If there exists a PII, contract will display a warning message and limit to the user.
4. Rules Contract: this smart contract has the rules for checking PII in the user data and return a limit or a warning message for particular PII.

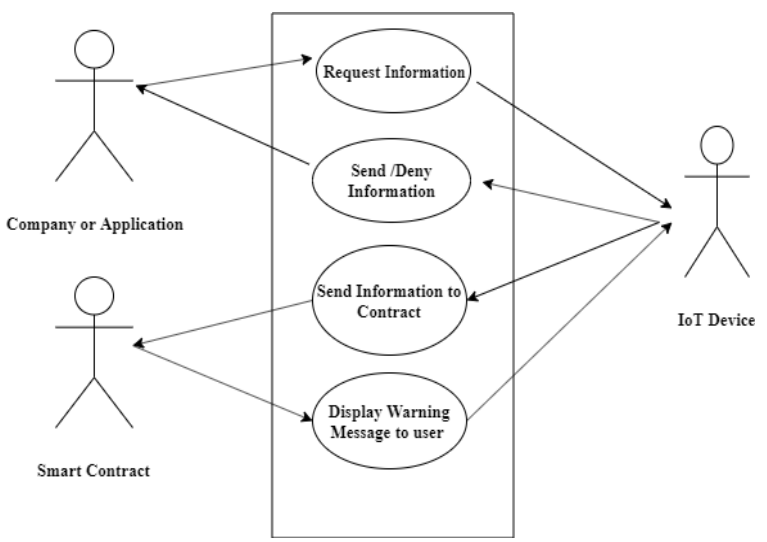
In the proposed model, after a company or application requests for information to be shared, the device will send that information to the data validation smart contract for the identification of personally identified information (PII). This contract will use the rules, smart contract, for checking PII in the user information, and it will return a limit and warning

message to the user if PII detected in the user information. This contract contains two more functions which are send-information and deny-information function. Sent-information function is used to share information and deny-information function is used to avoid sharing information with companies. The rules smart-contract includes a list of rules for detection of PII in the user information, for example, bank account number, social security number, Health care information, email address, etc. This contract contains three functions which are Add-rules, Delete-rules, and Search-rules. The Add-rules function is used to add new rules to the list Delete-rules function is applied to delete rules from the list and Search-rules function is utilized to search rules in the list.

Figure 2 shows the users interaction with the system, companies, smart contract and devices are interacting with each other through the system, to inform user for the risk of sharing personally identified information, the steps are defined below.

1. The Company or application requests personal information from the device.
2. The device sent that information to a smart contract for the identification of PII.
3. The smart contract identifies PII in the user information and sends a warning message to the user base on the PII.
4. Last, the user decides to send/deny information to the company.

Figure 2: Users Interaction with System



Source: Source: Author's Compilation

5 Algorithms for Data Validation Smart Contract

Algorithm: Data Validation

Input: information to be shared

Output: warning message

Required: connection with Rules smart contract

Function **Validate-Information** (information)

Check PII in the user information using rules from Rules smart contract

If PII found in the user information

Display warning message and limit of risk to user

End

Else

Display message with no risk

End

End

Algorithm: Send Information

Input: user information

Output: send user information

Required: the address of the receiver

Function **Send-Info** (Address r)

Send information to receiver

End

6 Algorithms for Rules Smart Contract

Algorithm: Addition of rules to the Contract

Input: Rule-id and Rule-description

Output: True/False

Function **Add-Rules** (Rule-id, Rule-description) only owner

If Rule-id and Rule-description are not present in the list of rules

Add Rule-id and Rule-description to the list of rules

Return true

End

Else

Rules already exist

Return false

End

End

Algorithm: Rules Deletion and Searching

Input: Rule-id

Output: True/False

Function **Remove-Rule**(Rule-id) only owner

If rule exist in the list of rules

Remove rule from the list

Return true

End

Else

The rule is not present in the list

Return false

End

End

Function **Search-Rules**(Rule-id)

If Rule-id is present in the list

Return true

End

Else

Return false

End

End

The smart contract provides several securities feature, in this work, the smart contract would alert users on the limit and risk of sharing personal information through a public network. The users have the right to decide whether to share or deny information on the public network. The contract has used the rules to identified PII in the user information base on the PII information user would be informed on the risk and limit of sharing PII information on the network. This work will reduce the privacy paradox in the IoT by giving the rights and alerts to the users on sharing PII information.

7 Performance Assessment and Transactions Costs

The purpose of our work is to design a smart contract to alert users on sharing PII information on a public network. For the testing of our proposed model, we have prototyped the smart contract in the solidity programing

language and deployed it on the Ropsten test network. The Ethereum network has charged, for the deployment of smart contracts and the execution of their functions. The following table includes the costs of smart contracts and their functions. The fixed costs of the deployment of a smart contract for Data-validation and Rules are 0.000494523 and 0.000594235, after the conversion to the dollar, the costs are respectively being 0.080 and 0.096. The cost of deployment is less than compared to the cost of function execution. The execution cost of the function is changeable base on input data, but the deployment cost is fixed.

Table 1: Charges of Smart Contracts and their Functions

Contracts and functions	Price per transaction	Price in ether	Price in USD $
Data-Validation	494523	0.000494523	0.080
Rules	150349	0.000594235	0.096
Validate-Information()	294352	0.000294352	0.047
Send-Info()	785600	0.00007856	0.013
Remove-Rule()	467340	0.000046734	0.0075
Add-Rules()	26357	0.000026357	0.0042

Source: Author's Compilation

8 Security Analysis

In this system, we integrate smart contracts and dynamic rules for the identification of personally identified information(PII) in the user's personal information. In the suggested system, users have full control over their records, and there is no chance for third parties to collect user's personal information without their permission. This system would alert users on sharing personal information on public networks and display the limit for PII information. The data-validation smart contract contains sent-info, deny-info, and validate-information functions these functions help the user to decide whether to share or deny information on the public network.

9 Conclusion

The results from the study of multiple literature reveal that a disparity between IoT users' intentions and behaviors regarding information privacy varies. Most people want to have personal data kept confidential by the system they decide to use while exhibiting actions that tend to compromise the privacy of personally identifying information. Multiple studies support the claims by providing interview findings that show people being willing to share personal information in exchange of money [16], [17]. The primary contributing factors of privacy paradox and fatigue is poor design of user interfaces, education levels, and social norms. One of the possible solutions

to the privacy paradox in IoT is the Implementation of smart contracts for alerts of the user. In this work, we implement a smart contract to evaluate personally identified information and inform users of the risk and limit of information sharing on the public network.

References

[1] M. Williams, J. R. C. Nurse and S. Creese, "The Perfect Storm: The Privacy Paradox and the Internet-of-Things," *2016 11th International Conference on Availability, Reliability and Security (ARES)*, Salzburg, 2016, pp. 644-652.

[2] Hargittai, Eszter; MARWICK, Alice. "What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy. International Journal of Communication, [S.l.], v. 10, p. 21, jul. 2016

[3] I. Pentina, L. Zhang, H. Bata and Y. Chen, "Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison", Computers in Human Behavior, vol. 65, pp. 409-419, 2016.

[4] R. Lee, S. Kiesler, R. Kang, M. Madden, M. Duggan, S. Brown, and L. Dabbish. "Anonymity, privacy, and security online." Pew Research Center 5 (2013).

[5] J. Carrascal, C. Riederer, V. Erramilli, M. Cherubini and R. de Oliveira, "Your browsing behavior for a big mac", Proceedings of the 22nd international conference on World Wide Web - WWW '13, 2013. Available: 10.1145/2488388.2488406 [Accessed 23 November 2019].

[6] I. Pentina, L. Zhang, H. Bata and Y. Chen, "Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison", Computers in Human Behavior, vol. 65, pp. 409-419, 2016.

[7] D. O'Neil, "Analysis of Internet Users' Level of Online Privacy Concerns", Social Science Computer Review, vol. 19, no. 1, pp. 17-31, 2001.

[8] C. Jensen, C. Potts and C. Jensen, "Privacy practices of Internet users: Self-reports versus observed behavior", International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 203-227, 2005.

[9] B. Stanton, M Theofanos, S. Prettyman and. S. Furman, "Security Fatigue", IT Professional, vol. 18, no. 5, pp. 26-32, 2016.

[10] Bada, Maria, Angela M. Sasse, and Jason R.C. Nurse. "Cyber security awareness campaigns: Why do they fail to change behaviour?." , 2019.

[11] BBC News, "Google agrees privacy policy changes with data watchdog," 2015.

[12] A. Dwivedi, G. Srivastava, S. Dhar and R. Singh, "A Decentralized Privacy-Preserving Healthcare Blockchain for IoT", Sensors, vol. 19, no. 2, p. 326, 2019.

[13] Li, Shancang, L. Xu, H. Song, and T. Chen. "Privacy, data assurance, security solutions for Internet of Things (PASS4IoT): Guest editorial." IET Networks 7, no. 5 2018.

[14] S. Paavolainen and P. Nikander, "Security and Privacy Challenges and Potential Solutions for DLT based IoT Systems," *2018 Global Internet of Things Summit (GIoTS)*, Bilbao, 2018, pp. 1-6

[15] M. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges", Future Generation Computer Systems, vol. 82, pp. 395-411, 2018.

[16] T. Li, C. Gao, L. Jiang, W. Pedrycz and J. Shen, "Publicly verifiable privacy-preserving aggregation and its application in IoT", Journal of Network and Computer Applications, vol. 126, pp. 39-44, 2019.

[17] H. Ren, H. Li, Y. Dai, K. Yang and X. Lin, "Querying in Internet of Things with Privacy Preserving: Challenges, Solutions and Opportunities," in *IEEE Network*, vol. 32, no. 6, pp. 144-151, November/December 2018.