INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE

ISSN: 2057-5688

CASH LESS SOCIETY: MANAGING PRIVACY AND SECURITY IN THE TECHNOLOGICAL AGE

RAYUDU VIJAYA LAKSHMI DURGA
PG Scholar, Department of M.C.A,
S.K.B.R P.G College,
Amalapuram, E.G.Dt., A.P, India.
Vijayalakshmidurgarayudu@gmail.com

Mr. NAGA. SRINIVASA RAO*
Asst. Professor, Dept of M.C.A,
S.K.B.R P.G College,
Amalapuram, E.G.Dt., A.P, India.
E-Mail:naagaasrinu@gmail.com

Abstract—

A cashless society is an economy that conducts financial transactions not in the form of traditional means of payment such as cash or coins, but through the transmission of digital data (usually through electronic means such as credit cards and mobile data) between the parties involved. Participants in a cashless society must find a way to protect their transaction data and recognize the risks that arise when organizations collect large amounts of this data, leading to a reduction in privacy. Balancing privacy and data security is critical in the information age, especially given the increasing risk of data breaches and exploitation. d Storage system via Deniable Attribute-based Encryption. To increase privacy in a cashless society, a few measures can be combined to produce a lasting and desirable outcome for users: a new type of banking service that assigns random numbers to credit cards, the use of blockchain to monitor all transactions by individuals and a campaign to educate and educate key stakeholders about security and privacy risks, to provide them with the tools and background knowledge needed to protect their own information before engaging with an unknown company or other third party (e.g., cybersecurity departments, IT technicians, etc.) .). Both blockchain and card number randomization are prone to zero-day errors, bugs, and differential social acceptance. This preliminary research relies on a systems analysis of cashless systems to identify and analyze a range of social and technical solutions to support a robust cashless system that protects user privacy and maintains system security. The information found and analyzed will be useful by revealing weaknesses in current methods of data integrity and security. Learning current and future methods of managing privacy and data security in the technological age would be helpful to take preventative countermeasures. This study provides important steps to prevent the loss of privacy in a cashless system.

***IndexTerms*—cashless, society, privacy, security, data, system**

I. INTRODUCTION

Systems are in a constant state of change, and their components must be updated to increase or maintain the ability to perform a task effectively and fulfill a purpose. The monetary system is complex and requires a thorough analysis of its components in order to function at an acceptable level. A cashless system is an economic condition in which all transactions are conducted without physical tender such as coins or paper bills. For a cashless system, privacy is a critical component to assess. Increasing privacy is and will remain a necessary endeavor in a cashless society. A majority of users are unaware of what type of data is collected about them and how that data is used. We thought the entire paper recognized the need to improve data protection and propose doing so with a three-pronged solution. First, promoting proper education about data collection and privacy will help people see the need for more privacy. Second, a randomized credit card scheme will help prevent unwanted parties from collecting sensitive and personal information about individuals. Third, blockchain will prove to be a powerful

ISSN: 2057-5688

authentication tool. Security is drastically improved by adopting these three approaches. Users will have more knowledge about the systems they use, hackers will have an extremely difficult time fooling the blockchain system and data, and it will be difficult to attribute them to specific individuals. A cashless society poses risks for its members as all their transactions are tracked online. Members of this cashless society must find a way to protect their transaction data or risk organizations collecting large amounts of data about them and compromising privacy.

II. RELATED WORK

The idea of a cashless society involves using digital-based technology to conduct transactions, which can range from buying a soda at the supermarket to transferring large amounts of money from one account to another. Digital transactions can be conducted through mobile applications, websites, credit or debit cards, and any other form of technology that will become prevalent in the future. The use of technology to conduct cashless transactions has become more widespread every decade since the 1940s [1].

CashlessTransactions

A. Immediately after World War II, citizens began using credit cards. The classic point-of-sale business only became widespread in the 1980s [2]. A point of sale transaction occurs when a customer swipes a card at a terminal to pay for a product or service. The terminal would read the magnetic stripe and confirm the required account information to complete the transaction. Swiping of cards with magnetic strips will be phased out in favor of cards with physically embedded chips. In 2000 PayPal was launched and allowed users to transfer money online. E-commerce site eBay uses PayPal to conduct transactions between users without having to involve personal bank account or credit card numbersIn 2009, Bitcoin revolutionized the world of currencies. This was an influential invention as it was the first form of a decentralized cryptocurrency. Anyone with an internet connection can get a bitcoin wallet, which contains a private key used to conduct transactions and customize wallet settings. Bitcoin exists outside of the jurisdiction of traditional banking systems, meaning it cannot be banned [1]. From 2010 to 2014 mobile payment apps such as Google Pay, Apple Pay and Venmo were introduced. Mobile payments allow users to make transactions using their mobile devices. Mobile phones started out as devices that could only make voice calls, but have evolved into powerful tools with functionality comparable to desktop computers. Mobile phones are becoming more and more powerful with more and more functions. With web-based applications available on mobile devices, online transactions have become easier and more convenient. As of 2017, PayPal processed 254 million customer accounts and 7.6 billion payments. The performance of mobile devices has contributed to this broad acceptance of the application [3].

A. ImportantConsiderations

Privacy and security must be considered with the increasing use of cashless transactions. Privacy is the state or condition of being free from observation or interference from other people. Data protection in the context of a cashless system includes protection against the involuntary collection and sorting of transaction information. Safety is the state of being free from danger or threat. Privacy and security are major concerns in a cashless society. Any gain in convenience would be nullified if people couldn't secure their money and personal information.

III. PRIVACYANDSECURITYCONCERNS

A. A system consists of elements, combinations of elements and a function or purpose [4]. A cashless society is a system made up of entities such as standard users, governments and banks. A cashless system provides a way to exchange digital currencies. Privacy and security concerns within a cashless system are numerous and need to be addressed.

B. TheCollectionofData

In today's totally cashless society, every transaction you make with your credit card is

ISSN: 2057-5688

stored in the appropriate merchant database. The information collected from customer transactions is used by all companies for accounting and tax purposes, but many of them collect large amounts of data about individuals. For example, when a person buys a product from Target, the store keeps a record of what that card bought [5]. This record is linked to that particular card and any other information Target may collect about that customer.As a result, people are unknowingly being exploited for the information they may not know they are divulging. The desired level of privacy would prevent a user from having their transactions collected and used unethically by companies and corporations. Any type of available data can be stored and sold if the quantity and quality of the data is useful for business or government applications. Data brokers collect and sell personal information about people. This information is often collected about individuals without their knowledge or express consent [5]. Today it is difficult to prevent data brokers from obtaining information about individuals. Almost everything people do is tracked in some way and used for other purposes. People may see this as an invasion of privacy. It is important to note that our daily lives are becoming less private.

EthicalConsiderations

Securing private data is especially important in places where governments and their agencies use data to draw inferences about citizens. Individuals can be linked to criminals in government databases because they meet certain criteria. Government agencies use data about people to find criminals [5]. If criminals typically buy certain products over a period of time, machine learning algorithms can detect this. If a non-criminal civilian buys a similar product during the same period, he could be identified as a potential criminal. By preventing the government agency from gaining access to large amounts of transaction data, innocent individuals could avoid being associated with criminals [6]. However, associations do not stop at criminal activities. Purchasing certain products with a certain frequency could be used by insurance companies and banks to identify people with medical conditions or bad debts. This complex scenario of what to do with all the data creates tensions between ethics and furthering business or government goals. Solutions need to be considered and implemented to address privacy concerns.

IV. SOLUTIONSANALYSIS

Solving the problem of limited privacy and security in a cashless society requires the implementation of new technological methods and the provision of valuable information to the public.

A. RandomizedCreditCardNumbers

To prevent stores and companies from collecting information about their customers, random card numbers can be used. When a customer using the randomized card system buys groceries from a store, the items purchased are linked to a specific card number. If the customer returns to the same store on another day with the same card, the purchase will be linked to a different card number than the day before. Figure 1 shows the difference between using a standard credit card and a randomized card in relation to a branch database. The database stores the real card number for standard credit cards and a different number for the randomized one.

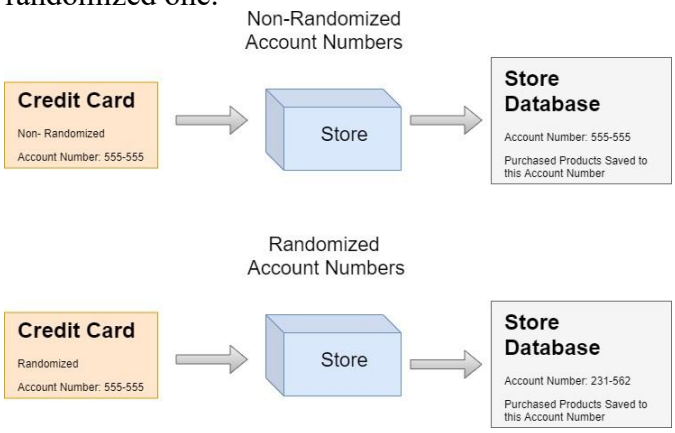

Figure1. TheRandomizedCreditCard

The randomized card system would behave similarly to a VPN (Virtual Private Network) used for Wi-Fi connectivity. When a mobile device tries to connect to a Wi-Fi signal without a VPN, it broadcasts its real Internet Protocol (IP) address [7]. On the other hand, a VPN allows the mobile device to send a proxy IP address, then

ISSN: 2057-5688

authenticate the network, and then give out its real IP address. However, the randomized credit cards work a little differently than VPN. The randomized credit card system consists of a primary account number mapped to randomized card numbers associated with individual transactions. If an account holder wants to check their transaction history, they can log into their bank's app or website and review their purchases in real time.

B. *Blockchain*

Another system that all levels of government will need to put in place will be a nationalized blockchain network that will handle transaction tracking in a secure and private manner. According to Melanie Swan's Blockchain: Blueprint for a New Economy, the blockchain acts as the public ledger of all transactions [8]. The blockchain contains complete information about each transaction and the data of each person involved in that transaction. This technology is more secure than other recording systems. The blockchain's ability to track in real-time allows for the elimination of error handling, which also allows for improved traceability. Such an achievement would first have to be created through the joint efforts of developers, engineers and designers. Regulations and operators/administrators can be set by legislators who first enact legislation dealing with who runs and maintains the secure blockchain network and moves the financial aspects of life onto the network.

C. *Implementation*

For the public to accept a randomized credit card scheme, users must either have an incentive to switch accounts or not switch at all. Incentives to switch accounts could be influenced by a publicly accepted need for more privacy. If the randomized credit card system is made the standard, any bank can adopt it and implement it for their users. This task will not be easy but would provide the best possible result for the users, which would mean more privacy and minimal hassle. In terms of blockchain, the features listed above provide more privacy and security for users who live and work in the U.S. To successfully introduce such changes into the modern financial system, education and outreach are vital. This phase focuses on the privacy and security aspects of a cashless society and aims to prepare prospective members for life after cash. A public awareness campaign would focus on acquiring and improving knowledge and understanding of current privacy laws and other practices related to finance. This policy-driven approach would primarily focus on preemptive privacy and security while increasing technological literacy among the population. Preemptive data protection can be defined as a customer decision that has a positive impact on the level of data protection and/or the security of their data (before implementing strategies such as blockchain and other forms of encryption). In 2019, there were 1,473 data breaches, with 164,683,455 records containing sensitive data being released [9]. Although this statistic is lower than last year, it's still important to emphasize the importance of protecting personal data and the reality of vulnerabilities in the security of private information. By first bringing more power and autonomy into society, the flow of information will increase, dispelling most of the uncertainty and mistrust in a cashless system. According to Donella Meadows, one of the main causes of system failure is a lack or disruption in the flow of information [10].By providing a source of knowledge and transparency for those who may not be as experienced with electronic forms of payment, this system would teach people how to properly manage their own privacy while maintaining current privacy and security measures. By sharing responsibility with the user, companies and other entities with greater power can place greater focus on the products or services they offer. Minimizing human error will allow greater effort to be devoted to more serious cybersecurity risks and issues. Although large organizations will most likely see a decline in data collection and analysis, more attention can be focused on strengthening current cybersecurity measures and protecting one

ISSN: 2057-5688

of their most important economic assets: the customer. Large organizations that process, store and manage transactions (shops and banks) would benefit if their users were responsible about their privacy and security. Data breaches cost businesses millions of dollars. In 2019, the average cost of a data breach for a US-based company was $8.19 billion [11]. Ideally, by increasing user accountability for large organizations that are entrusted with valuable data, they can be more vigilant about their own security risks and gaps within databases and firewalls.

V.PREDICTIVEANALYSIS

A cashless system consists of many different elements. Each element can react differently to changes. Analyzing potential solutions[12], to a problem can provide helpful insights into how their application affects the system.

UsingBlockchain

Currently, physical safes storing cash in consumer banks and federal banks are at risk of robbery and damage. With a blockchain network, there would be secure, encrypted confirmations of money flow. There is no risk of burglary due to the existing level of security that combines manpower and machinery.

UsingaRandomizedCardSystem

Credit cards are vulnerable to skimming devices that can be strategically placed on real working scanners to scan and store sensitive credit card related data. A randomized card scheme helps alleviate this problem by assigning a randomized credit card number to the stolen or imported card and adding an extra security measure that in turn eliminates fraud-related problems that banks deal with on a daily basis.

SocialResponsibilityandAwareness

Public confidence in knowing and managing their own financial privacy is critical to the future development and popularity of cashless payment methods. With the trend towards a completely cashless society, it is important that users have the knowledge, experience and logical understanding to protect their own information. Promoting technological literacy through educational and promotional campaigns would ease some of the burdens tech companies and service providers have to bear. Awareness of the risks associated with a cashless society would reduce many ignorance-caused problems that people face regarding security and experience the protection of their financial and personal data.

TheTechnologicalProgression

With a credit card randomization system and a nationalized blockchain network, it increases user privacy and security. Rather than replacing current means of financial transactions, such a measure would complement these day-to-day spending activities and habits. As transactions are conducted, all data associated with those transactions is kept secure either through randomized credit card numbers or the enhanced real-time traceability of the blockchains.

A. Implications

An economic implication of the establishment of a nationalized blockchain network is that the demand for human labor in financial institutions is likely to decrease, leading to a societal shift towards computer-based interactions. This is a likely scenario as the system will verify each transaction and will be able to send, receive and process messages and deal with large numbers of fraudulent transactions, saving time for credit card companies, banks and ultimately lawyers.

B. FittingintoSociety

It is normal for a society to fear something it does not understand or that seems foreign to its traditions. A cashless society may initially be opposed by both the political right and the left. If the situation surrounding Facebook and British policy consultancy Cambridge Analytica has taught the world one thing, it's that lawsuits can be the key to stronger privacy protections in the United States. Facebook's suspension of Cambridge Analytica was a scandal in which the consulting firm abusively acquired the data of 50 million Facebook users in 2014-2015, which was

then used in Donald Trump's then presidential campaign. Society will quickly realize that new technologies are necessary for their everyday lives, because with every day that goes by without them, companies can collect more data and have more control over their lives.

VI. CONCLUSION

A cashless society poses risks for its members as data and metadata about their transactions are collected and used. Members of this cashless society must find a way to protect their data in order to increase their privacy. Our group has found that the idea of a cashless society involves many systemic complexities. Within the complex system, there are opportunities to implement solutions for data protection and security issues. The different actors in this system have different desires and respond in unique ways to changes made. Sometimes the best solution to a problem is the culmination of multiple approaches. Disseminating information to the general public helps people learn more about the systems they use and empowers them to make informed decisions. Blockchain helps promote privacy and security through its authentication process. Randomized credit cards help users keep their account numbers private. All three approaches are effective ways of adapting to a dynamic monetary system.

REFERENCES

1. Improving product marketing by predicting early reviewers on E-Commerce websites
S. Kodati, M. Dhasaratham, V. V. S. S. Srikanth, and K. M. Reddy, "Improving product marketing by predicting early reviewers on E-Commerce websites," Deleted Journal, no. 43, pp. 17–25, Apr. 2024, doi: 10.55529/ijrise.43.17.25.

2. Kodati, Dr Sarangam, et al. "Classification of SARS Cov-2 and Non-SARS Cov-2 Pneumonia Using CNN." Journal of Prevention, Diagnosis and Management of Human Diseases (JPDMHD) 2799-1202, vol. 3, no. 06, 23 Nov. 2023, pp. 32–40, journal.hmjournals.com/index.php/JPDMHD/article/view/3406/2798, https://doi.org/10.55529/jpdmhd.36.32.40.

3. V. Srikanth, "CHRONIC KIDNEY DISEASE PREDICTION USING MACHINE LEARNING ALGORITHMS," IJTE, pp. 106–109, Jan. 2023, [Online]. Available: http://ijte.uk/archive/2023/CHRONIC-KIDNEY-DISEASE-PREDICTION-USING-MACHINE-LEARNING-ALGORITHMS.pdf

4. V. SRIKANTH, "DETECTION OF PLAGIARISM USING ARTIFICIAL NEURAL NETWORKS," International Journal of Technology and Engineering, vol. XV, no. I, pp. 201–204, Feb. 2023, [Online]. Available: http://ijte.uk/archive/2023/DETECTION-OF-PLAGIARISM-USING-ARTIFICIAL-NEURAL-NETWORKS.pdf

5. V. SRIKANTH, "A REVIEW ON MODELING AND PREDICTING OF CYBER HACKING BREACHES," IJTE, vol. XV, no. I, pp. 300–302, Mar. 2023, [Online]. Available: http://ijte.uk/archive/2023/A-REVIEW-ON-MODELING-AND-PREDICTING-OF-CYBER-HACKING-BREACHES.pdf

6. S. Kodati, M. Dhasaratham, V. V. S. S. Srikanth, and K. M. Reddy, "Detection of fake currency using machine learning models," Deleted Journal, no. 41, pp. 31–38, Dec. 2023, doi: 10.55529/ijrise.41.31.38.

7. "Cyberspace and the Law: Cyber Security." IOK STORE, iokstore.inkofknowledge.com/product-page/cyberspace-and-the-law. Accessed 2 May 2024.

8. "Data Structures Laboratory Manual." IOK STORE, www.iokstore.inkofknowledge.com/product-page/data-structures-laboratory-manual. Accessed 2 May 2024.

ISSN: 2057-5688

9. Data Analytics Using R Programming Lab." IOK STORE, www.iokstore.inkofknowledge.com/product-page/data-analytics-using-r-programming-lab. Accessed 2 May 2024.

10. V. Srikanth, Dr. I. Reddy, and Department of Information Technology, Sreenidhi Institute of Science and Technology, Hyderabad, 501301, India, "WIRELESS SECURITY PROTOCOLS (WEP,WPA,WPA2 & WPA3)," journal-article, 2019. [Online]. Available: https://www.jetir.org/papers/JETIRDA06001.pdf

10. V. SRIKANTH, "Secured ranked keyword search over encrypted data on cloud," IJIEMR Transactions, vol. 07, no. 02, pp. 111–119, Feb. 2018, [Online]. Available: https://www.ijiemr.org/public/uploads/paper/1121_approvedpaper.pdf

11. V. SRIKANTH, "A NOVEL METHOD FOR BUG DETECTION TECHNIQUES USING INSTANCE SELECTION AND FEATURE SELECTION," IJIEMR Transactions, vol. 06, no. 12, pp. 337–344, Dec. 2017, [Online]. Available: https://www.ijiemr.org/public/uploads/paper/976_approvedpaper.pdf

12 . SRIKANTH MCA, MTECH, MBA, "ANALYZING THE TWEETS AND DETECT TRAFFIC FROM TWITTER ANALYSIS," Feb. 2017. [Online]. Available: http://ijmtarc.in/Papers/Current%20Papers/IJMTARC-170309.pdf

14 Srikanth, V. 2018. "Secret Sharing Algorithm Implementation on Single to Multi Cloud." International Journal of Research 5 (01): 1036–41. https://journals.pen2print.org/index.php/ijr/article/view/11641/11021.

5. K. Meenendranath Reddy, et al. Design and Implementation of Robotic Arm for Pick and Place by Using Bluetooth Technology. No. 34, 16 June 2023, pp. 16–21, https://doi.org/10.55529/jeet.34.16.21. Accessed 20 Aug. 2023.

16. Babu, Dr P. Sankar, et al. "Intelligents Traffic Light Controller for Ambulance." Journal of Image Processing and Intelligent Remote Sensing(JIPIRS) ISSN 2815-0953, vol. 3, no. 04, 19 July 2023, pp. 19–26, journal.hmjournals.com/index.php/JIPIRS/article/view/2425/2316, https://doi.org/10.55529/jipirs.34.19.26. Accessed 24 Aug. 2023.

17. S. Maddilety, et al. "Grid Synchronization Failure Detection on Sensing the Frequency and Voltage beyond the Ranges." Journal of Energy Engineering and Thermodynamics, no. 35, 4 Aug. 2023, pp. 1–7, https://doi.org/10.55529/jeet.35.1.7. Accessed 2 May 2024.

18. K. Meenendranath Reddy, et al. Design and Implementation of Robotic Arm for Pick and Place by Using Bluetooth Technology. No. 34, 16 June 2023, pp. 16–21, https://doi.org/10.55529/jeet.34.16.21. Accessed 20 Aug. 2023

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688