The Safety of RFID Users' Privacy by Blocking Hackers From Masking Their Tags

Bharanitharan A/L Visvanathan
School of Computing
Asia Pacific University of Technology and innovation (APU)
Kuala Lumpur, Malaysia
TP056319@mail.apu.edu.my

Dr. Intan Farahana Binti Kamsin
School of Computing
Asia Pacific University of Technology and innovation (APU)
Kuala Lumpur, Malaysia
intan.farahana@staffemail.apu.edu.my

***Abstract*- In this technological era, RFID systems have evolved in the ways we didn't see coming. This research shows all the privacy and security advancements of this app. It also covers the difference between the old secure system and the new one which has been implemented. Users can login to the app and proceed with many services such as top up, bill payments, transfers, and many more. They can do it peacefully by knowing that their details are safe and secured. This is because, this data is accessed over an external server, such as the Internet, security and privacy are important issues whenever it is accessed. The findings of this research will show you that this proposed system is very advanced, user-friendly and secured at the same time.**

Keywords— Security, Masking, Biometrics, RFID tag.

I. INTRODUCTION

Radio frequency identification technology has advanced from obscurity to mainstream applications that aid in the acceleration of the handling of produced items and materials in recent years. RFID permits remote identification, and unlike previous bar-code technologies, it does so without requiring a line of sight. RFID tags may store a greater number of unique identifiers than barcodes and can also include extra data such as manufacturer, product kind, and even environmental parameters such as temperature. Additionally, RFID systems are capable of recognising many tags that are situated in the same general region without the intervention of humans. Consider a supermarket checkout counter, where each bar-coded item must be oriented toward the reader prior to being scanned. Many types of RFID exist, but at the highest level, we can divide RFID devices into two classes: active and passive. One of the most exciting features of current RFID tags is their ability to send information that goes beyond data stored in an internal memory to include data generated dynamically by onboard sensors. Commercially available RFID technology is currently capable of ensuring that important environmental limits are not exceeded (Want, 2006).

There are a lot of privacy issues for the users of RFID tags. Despite its promise, RFID confronts certain obstacles when applied to the Internet of Things. The majority of security and privacy concerns stem from a breach of the air interface between a tag and its reader. Numerous security researchers have written articles assessing the biggest dangers to RFID technology and examining alternative strategies for protecting privacy and ensuring its integrity.

Blocking occurs when an attacker uses a blocker tag to generate a large number of tags and causes a denial of service condition when the reader attempts to interrogate these non-existent tags. Jamming is a term that refers to the act of paralysing a communication system by creating radio noise at the same frequency as the system. Early detection and localization of blocking and jamming devices enables necessary action to be taken. The RFID system is composed of the following components: tag, air interface, reader, network, and back-end. One or more of these components may be targeted by a threat. Due to the increase of threats to RFID data, it is critical to safeguard the data's confidentiality (C), integrity (I), and availability (A). Threats to RFID data can affect it in three ways. The study will identify the threat, the RFID component(s) that are affected, and the impact on the data, before mitigating the risks using approved procedures (Khoo, 2011).

The system which is proposed will have various ways to overcome the problems stated above. One of the ways is by using blocker tags. Blocker tags were initially proposed to preserve users' privacy and to prevent unwanted readers from successfully interrogating neighbouring tags. It was first developed and introduced by Jules et al. on the basis of the binary tree walking singulation technique, but the study notes that this concept can be applied to ALOHA-based singulation approaches as well (Vahedi et al., 2011).

II. LITERATURE REVIEW (RESEARCH DOMAINS)

A. Safety in Cybersecurity

The Internet of Things (IoT) is a ground-breaking new technology that has transformed the worldwide community of contacts, smart devices, smart things, data, and knowledge. The Internet of Things is still very much in infancy, and numerous obstacles remain unresolved. The Iot technology is a unified notion that encompasses all aspects of life. The Internet of Things offers enormous potential for enhancing the worlds largest access, authenticity, reliability, scale, privacy, and interoperability. Securing IoT, on the other hand, is a complex issue. System security is crucial for the Internet of Things' development. This article provides an in-depth examination of IoT cybersecurity. The paradigm is defined by its ability to safeguard and integrate diverse connected devices and data communications technology (ICT). Our review is useful to anybody interested in IoT cybersecurity, since it discusses latest research, IoT cybersecurity design and taxonomies, critical supporting countermeasures and strategies, major industry applications, and research trends and barriers (Lu & Xu, 2019).

Safety and cybersecurity protection are vital for the smooth and dependable of modern intelligent automation, many of which provide mission-critical activities and services. Because it is well recognised that safety and protection are inextricably intertwined, they should be addressed continuously in such systems. As a result, several approaches to co-engineering security and cybersecurity in intelligent systems have been presented. This article provides an in-depth examination of co-engineering approaches for safety and information security, as well as relevant open problems and research concerns. Despite the breadth of available research, some crucial issues remain unanswered (Kavallieratos et al., 2020).

Education is both a means and an end in itself for the development of society and its contributions to human resources, well-being, and prosperity. Security and privacy concerns are ingrained in academic system as a result of several violent and terrorist incidents. While technologies have indeed been deployed to improve the quality of learning, both inside and outside of schools, security has been neglected. The fully unified technologies have been applied through the use of intelligent monitoring and sensing equipment. The primary objective of this study is to explore Internet of Things (IoT) options designed specifically for educational settings with the goal of developing smart and secure systems. Additionally, this article discusses a Secure Internet of Things for Smart Schools (S-IoST) that is built on a new sophisticated communication system that integrates 5G cellular systems, sensor technologies, intelligent transport systems, and IoT network (Qureshi et al., 2021).

Brain-computer interface BCI is a real-time communication technology that connects the brain to external devices. The BCI system can immediately convert the information provided by brain into commands that can be utilised to operate external equipment and act in place of human limbs or speech organs, empowered efficient communication of the external world. In other words, the BCI system can serve in place of normal periphery nerve and muscle tissue to enable interaction between a human and a computer, as well as between a person and the external environment. The goal of this work is to aid network security professionals in safely recognising brain processes in real time for BCI applications. To accomplish this, we proposed the construction of an RFID-based system in which semi-active RFID tags put on the scalp outside the brain wirelessly communicate collected activity in the brain to a device SC (Scanner Controller) equipped with a micro and timer integrated for each patient. Additionally, the study developed a novel prototype system interface named the BCI Identity System (BCIIS) to assist the patient during the identification operation. We reasoned that, enjoying the value of RFID, if the concept is effectively implemented by business, it has the order to enhance and protect BCI systems (Ajrawi et al., 2021).

Based on the research done for this specific domain, we can see that there are many ways of safety in cybersecurity to keep hackers away from accessing the tags and we can even use far more advanced safety features in the upcoming system.

B. RFID user's privacy

This magazine analyses how RFID technology is perceived as a danger to privacy in the setting of the earliest RFID deployments by major retailers across Europe And north America. Our contribution attempts to identify early in the risk creation process strategic techniques through which RFID providers and users might positively impact public acceptance of the technology. Based on study findings on risk perception and technical adoption, we provide a strategic framework for addressing public views of RFID-related privacy concerns, as well as a set of options for resolving peoples opinion of RFID-related privacy concerns (Thiesse, 2007).

RFID technology, that is used to identify objects and people and automatically incorporates context data such as the user's location, is expected to become a crucial and essential component of ubiquitous infrastructure. This technology has been implemented in a variety of sectors, including context of retail management. Recently, the number of research studies on mobile RFID has increased, which provides RFID services to the users via a reader integrated into their mobile device. However, there is rising concern, and even some opposition, regarding the tracking and profile of users via RFID technology. As a result, we assess privacy issues that have been documented in a variety of RFID applications and identify some new concerns about privacy in mobile RFID that are impeding its progress. Additionally, we investigate if various privacy-protection mechanisms established for RFID may be extended to mobile RFID (Hyangjin Lee & Jeeyeon Kim, 2006).

This article sums up recent technical studies on radio frequency identification's privacy and security implications (RFID). RFID tags are extremely small, wireless devices that facilitate the identification of objects and persons. They are expected to proliferate into the billions, if not trillions, during the next several years as a result of cost reductions. RFID tags are used to track goods throughout supply chains and are increasingly being embedded in customers' pockets, belongings, and even body. This survey examines scientific ways to ensuring the privacy and integrity of RFID systems, and the social and technical environments in which they operate. While the poll is intended for non-specialists, this may serve as a guide for experts (Juels, 2006).

Based on the research done on this specific domain, the privacy of RFID users has not been protected fully. Therefore, by improving the security of the upcoming system this privacy issue will be solved.

C. Identity Theft

Identity theft is feasible due to the nature of current payment methods. Vendors are willing to promote goods and services to strangers in return for a promise to pay, as lengthy as the promise is backed up with data connecting the buyer to a particular account or credit history. Identity theft comprises acquiring sufficient information about another person to create a false relationship, allowing the thief to purchase things using another person's credit card. Naturally, the card payment system is defined for decades by anonymous data-based operations (Anderson et al., 2008).

The growth of online commercial transactions has resulted in an increase in identity theft instances, which has resulted in significant financial losses for both customers as well as the e-commerce industry. Identity theft is a big issue for both

organisations and individuals on the internet. While the practical significance of preventing identity theft has sparked public interest, scientific study on the subject is scant. Based on coping behaviour theories, this study examines two types of coping behaviours used to combat identity theft. We validate the model utilizing data collected via a survey from 117 persons. The data indicate that both old and new techniques of coping are good at stopping identity theft (Lai et al., 2012).

We examine how easy it would be for a possible threat to conduct automated crawl and identity theft attacks against a range of popular social media platforms in order to get a sizable amount of personal user data in this article. The first assault we'll demonstrate is automatic identity theft from current profile pages, followed by the cloned victim's contacts receiving friend requests. According to the attacker, the contacted individuals should just trust and approve the friend request. By establishing friendships with the contacts of a victim, the attacker has access to the victim's sensitive information. In the second, more advanced strategy we present, we show that an automatic, cross-site profile clone attack is effective and feasible. We can immediately create a forged profile on a network in which the victim is not yet a member and approach the victim's friends who really are members of both networks involved in this assault. According to our testing results with real users, the automatic attacks we give are successful and realistic (Bilge et al., 2009).

Identity theft cost businesses and individuals $56 billion in the United States in 2005, with company data breaches responsible for up to 35% of reported identity thefts. Numerous states have responded by passing general data protection laws, which require firms to notify customers in the event of a data breach. Although the limits are intended to reduce identity theft, their impact has not been quantified. Using data over the period from the US Federal Trade Commission, we examine the influence of data breach disclosure requirements on identity theft from 2002 to 2009. We discovered that requiring data breach disclosure reduces identity theft caused by data breaches by an average of 6.1 percent (Romanosky et al., 2011).

Based on the research above, identity theft is happening very easily nowadays. Therefore, the upcoming system should have double layer masking and security to prevent the RFID tags from getting hacked.

III. SIMILAR SYSTEM

A. *Touch n'Go eWallet*

Touch 'n Go eWallet is a smartphone application with a built-in wallet. A actual Touch 'n Go Card is used. Users can enter their Physical Touch 'n Go card number into the app to track their transactions more easily. The following are some of the other features available in the app to make daily use easier. Firstly, Send money to other Touch 'n Go eWallet users. Secondly, Reload mobile prepaid. Thirdly, Pay for utilities and post-paid bills. Next, Purchase movie and flight tickets and dynamic QR code payment at participating Touch 'n Go eWallet retailers. Lastly, Pay tolls using RFID and TNG Card. An instrumental evaluation determines how an application contributes to or is successful in achieving a goal (Hussain et al., 2021).

Fig. 1. Touch n'Go eWallet app

B. *Samsung Pay app*

Samsung Pay is a new way to make purchases on Samsung's most recent smartphone models. The idea is to use most technology in almost all purchases.

Samsung Pay, on the other hand, might make use of near-field communication (NFC) technology. Samsung uses tokenization, a "new" complex alphanumeric method. Samsung accepted the VTS architecture (Visa Token Service) to promote its ambitious project, partnering with card providers such as Visa, Mastercard, and others. If you use Samsung Pay, you probably aren't thinking about the company's new market expansion plans. For example, online purchases or memberships that can be customised. In the electronic market, Samsung took a stride forward. As a result, the process of purchasing it is quite exciting. When a user adds a card to Samsung Pay, the system creates a new "virtual random" CC, which implements the framework that allocates a token to each card. This procedure is based on the Spayfw package. That token, along with the original PAN information, is preserved in a Token Vault. Instead of sending the original CC data with each transaction, the system sends a tokenized number: a new card number with certain "parameters" in the tracks. The key notion is that if someone obtains a token, he or she will be unable to reuse or extract information from the original CC (Son et al., 2015).

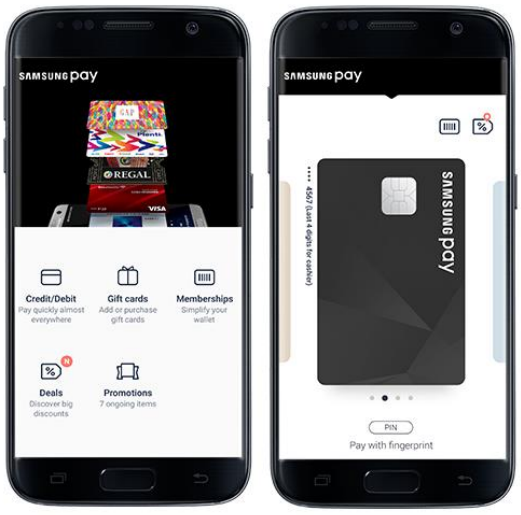

Fig. 2. Touch n'Go eWallet app

TABLE I. SIMILAR SYSTEMS

Criteria / Similar Systems	Touch 'n Go	Samsung Pay
Mobile app	/	/
Cloud		/
Multiple services provided	/	/
2-factor-authentication	/	/
Uses users Camera	/	

C. Summary

Both applications display a number of criteria that are present in the two similar systems; nevertheless, in order to produce a superior app, all of the features or criteria mentioned in the proposed app will be presented. To begin, both programmes are mobile-based and store user databases, making database management and organisation easier. In addition to the present functionalities, the app would include a biometric security feature (fingerprint password) to protect the security of user data. It will also have a number of safeguards in place to prevent hackers from gaining access to the tags.

IV. PROBLEM STATEMENT, AIMS AND OBJECTIVES

An RFID tag is made up of a small integrated circuit and a small transmitter that can communicate a unique serial number to a reading device across a distance of several metres in response to a query. The majority of RFID tags are passive, meaning they do not have batteries and get their power from the query signal (Juels et al., 2003). A reader and numerous tags make up a standard RFID system. The reader recognises things using wireless communications and tags affixed to the objects, each of which has its own unique ID (Yuan-Cheng Lai & Chih-Chung Lin, 2009).

The public is concerned about a number of issues, including privacy. Certain customers are concerned about being monitored by other readers when carrying RFID-tagged items. RFID tags can be used to retrieve personal details such as the kind of clothing worn by an individual, the brands in which an individual is interested, or information about a peron carrying an RFID-embedded bottle of medication, in addition to tracking individuals. Certain malicious organization or dealers may use RFID tags to sell fake RFID-embedded things and misrepresent them as valuable commodities (Yuan-Cheng Lai & Chih-Chung Lin, 2009). Another type of issue that attackers attempting to interrupt an RFID-based system can create is a denial of service assault (DoS). Additionally, certain RFID applications require unique considerations. For example, Molnar and Wagner outlined the challenges that should be considered while designing RFID-enabled libraries. Juels and Pappu consider the security concerns associated with the use of RFID technology in RFID-enabled bank notes (Vahedi et al., 2011).

One of the ways to overcome this issue is blocker tags. For privacy protection, use a blocker tag strategy. Blocker tags selectively abuse the tree-walking singulation mechanism, as demonstrated. The blocker tag does not participate in active jamming. Rather, it executes a kind of passive jamming by engaging in the tag-reading process in a non-compliant (or, more precisely, super compliant) manner (Lai & Lin, 2012).The blocker tag simulates the entire range of possible tag serial numbers, masking the serial numbers of other tags. By requiring it to sweep the whole space of all potential tag identifiers, which is incredibly huge, the blocker tag successfully overwhelms this operation (Yuan-Cheng Lai & Chih-Chung Lin, 2008).

The aim of this research is to develop an application which detects if any reader is accessing your cards and will jam the tag immediately. Thus, it will also provide a better protection of the RFID tag where the information of the individuals will not be hacked and exposed. While the objective of the research is:

- To develop blocker tags as a privacy tool for the application.
- To avoid hackers from getting access to RFID.
- To secure the users data from being exposed.

This research is conducted to help RFID users regarding the safety of their tags and to make it more secure. Through this app users will be able to always be a step ahead when it comes to the security of their tags. To ensure the security of the RFID tags the individuals have to follow the rules and regulations of the application. This application has a security layer to keep the data contained. Users simply have to sign up for the time and fill in the required details. After that they can proceed to login daily. There are two different solutions to overcome the RFID tag issue. These solutions can be classified into two categories. For RFID security, the first group employs blocking, jamming, and physical methods. Cryptographic principles and security methods are used by the other group.

V. METHODOLOGY

A. Sample Size

A total of 100 people will participate in the survey, including app developers, tag users, creators, and residents. In the future, the responses evoked by this group of people can be analysed and improved upon.

B. Data Collection Method

Because the results can be utilised to develop the app, questionnaires were employed to collect data in this study. Additionally, it is critical to deliver questions in an understandable manner so that respondents from diverse backgrounds can participate. Respondents will receive surveys by email, and the same will be true for answer retrieval; this will save both parties money and time, while also being more ecologically friendly. The survey form contains ten multiple-choice questions and one objective question in which respondents are asked to suggest ways to improve the functionality of the app. An examination of the proposed system's qualities and feasibility would be undertaken using the survey's facts and figures, allowing consumers to have firsthand knowledge with how it operates. The effectiveness, reliability, appropriateness, and usability of the proposed system are all evaluated (Lai & Lin, 2012).

C. Sample Case

The reasoning of sampling cases differs significantly from that of statistical sampling. The purpose of theoretical sampling in case studies is to select cases that are likely to replicate or extend the emergent theory, as well as to fill theoretical categories and offer examples for polar kinds. As a

result, whereas quantitative sampling is concerned with representativeness, qualitative sampling is concerned with information richness and selects examples systematically rather than randomly (Yuan-Cheng Lai & Chih-Chung Lin, 2009).

D. Identify Respondents

RFID tag users, tag producers, and citizens are among the study's participants. Because they are more likely to understand how the app's data storage and security mechanism will function. On the contrary, civilians are included as respondents in the study because the topic at hand necessitates anybody with an RFID tag to speak up about their consumer experiences (Yuan-Cheng Lai & Chih-Chung Lin, 2008).

Figure 3 shows the first part of the proposed system. Once the user starts the app, they will be directed to the login page. Here they can create a new account for the first time users and those who have already created can login. There is a feature which will lock the app until they have logged in. Once they click "Create Account", they simply have to follow the app's instructions. Firstly, insert the phone number which was registered to the RFID tag. Then an OTP code will be sent to that number for verification. If the number isn't verified they will be redirected to the login page. On the other hand, once the number is verified they can register their RFID tag and proceed to Fingerprint password session. After the fingerprint is set, their account is created. In this case, next time when they launch the app they can straight log in and continue.

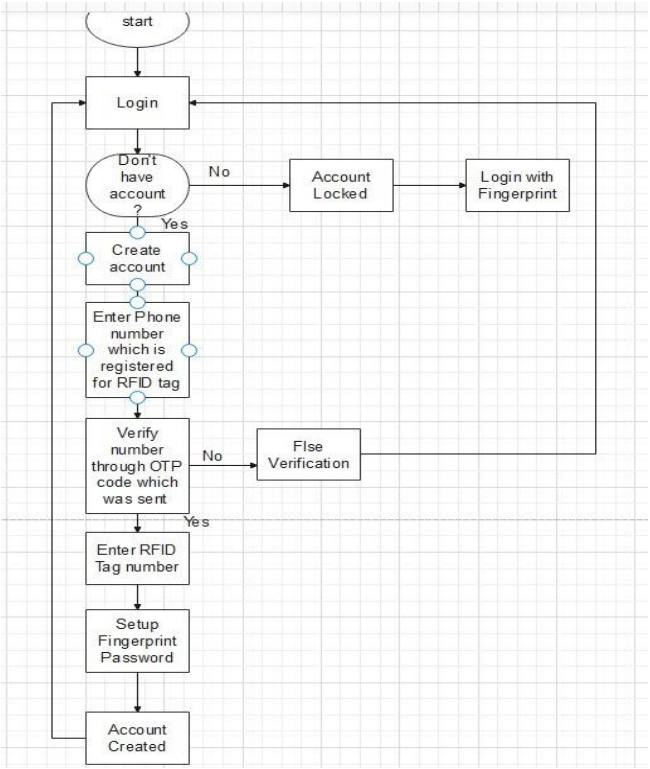

Fig. 3. App Registration and Login Process

As shown in Figure 4, once the user has created their account, they will be given this menu. In this case, the user can make bank services, top up services, remittance services, pay their bills and settings.

Bank Services

Users can make wallet transfers, bank transfers, check their account balance, and make payment for merchandise. This is because the bank card which was registered for the RFID tag will be transferred here automatically once the Account is created.

Top up Services

Users can top up their mobile number, internet, and toll.

Remittance Services

Users can send money to anyone whether it's domestic or international.

Bill Pay

Users can pay their electricity, tol, tax, loan, and fee bills through this app.

Settings

In this section, users can change their passwords. When they change their password, they have to go through the authentication process once again.

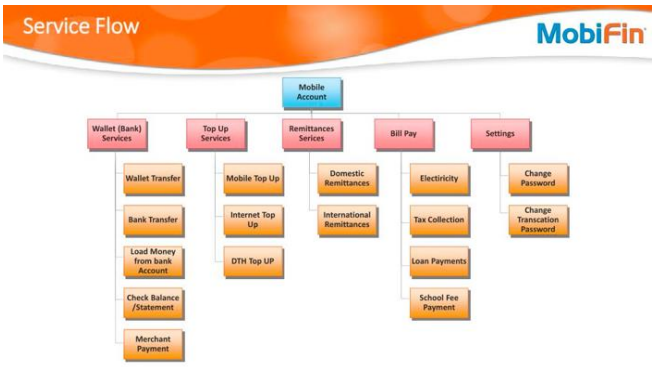

Fig. 4. Main Page

I. CONCLUSION

In this research, we suggest using fingerprint passwords as biometric-based authentication for keeping the users data safe. The proposed system has two different parts. First part is the login and authentication. Whereby, the second part is the menu provided for the user. Fingerprint passwords are an interesting and exciting area that has gained a lot of attention in recent years. This app also includes tons of benefits such as payments, transfers, top up services, bill management and many more. All of the above are very important and personal data so it will be protected well by this app. This app is built with all the latest recommendations. Therefore, there will be no changes to make now. However, in the future, the technology may evolve and new various systems might be introduced. Therefore, those can be added and updated when it's needed.

References

Yuan-Cheng Lai, & Chih-Chung Lin. (2009). Two blocking algorithms on adaptive binary splitting: Single and pair resolutions for RFID Tag Identification. *IEEE/ACM Transactions on Networking*, *17*(3), 962–975. https://doi.org/10.1109/tnet.2008.2002558

Yuan-Cheng Lai, & Chih-Chung Lin. (2009). A blocking RFID anti-collision protocol for quick tag identification. *2009 IFIP International Conference on Wireless and Optical Communications Networks*. https://doi.org/10.1109/wocn.2009.5010553

Yuan-Cheng Lai, & Chih-Chung Lin. (2008). A pair-resolution blocking algorithm on adaptive binary splitting for RFID tag identification. *IEEE Communications Letters*, *12*(6), 432–434. https://doi.org/10.1109/lcomm.2008.080056

Vahedi, E., Shah-Mansouri, V., Wong, V. W., Blake, I. F., & Ward, R. K. (2011). Probabilistic analysis of blocking attack in RFID systems. *IEEE Transactions on Information Forensics and Security*, *6*(3), 803–817. https://doi.org/10.1109/tifs.2011.2132129

Lai, Y.-C., & Lin, C.-C. (2012). Two couple-resolution blocking protocols on adaptive query splitting for RFID Tag Identification. *IEEE Transactions on Mobile Computing*, *11*(10), 1450–1463. https://doi.org/10.1109/tmc.2011.171

Juels, A., Rivest, R. L., & Szydlo, M. (2003). The blocker tag. *Proceedings of the 10th ACM Conference on Computer and Communication Security - CCS '03*. https://doi.org/10.1145/948109.948126

Lu, Y., & Xu, L. D. (2019). Internet of things (IOT) cybersecurity research: A review of current research topics. *IEEE Internet of Things Journal*, *6*(2), 2103–2115. https://doi.org/10.1109/jiot.2018.2869847

Kavallieratos, G., Katsikas, S., & Gkioulos, V. (2020). Cybersecurity and safety co-engineering of Cyberphysical Systems—a comprehensive survey. *Future Internet*, *12*(4), 65. https://doi.org/10.3390/fi12040065

Qureshi, K. N., Naveed, A., Kashif, Y., & Jeon, G. (2021). Internet of things for education: A smart and secure system for Schools Monitoring and alerting. *Computers & Electrical Engineering*, *93*, 107275. https://doi.org/10.1016/j.compeleceng.2021.107275

Ajrawi, S., Rao, R., & Sarkar, M. (2021). Cybersecurity in brain-computer interfaces: RFID-based design-theoretical framework. *Informatics in Medicine Unlocked*, *22*, 100489. https://doi.org/10.1016/j.imu.2020.100489

Thiesse, F. (2007). RFID, privacy and the perception of risk: A strategic framework. *The Journal of Strategic Information Systems*, *16*(2), 214–232. https://doi.org/10.1016/j.jsis.2007.05.006

Hyangjin Lee, & Jeeyeon Kim. (2006). Privacy threats and issues in Mobile RFID. *First International Conference on Availability, Reliability and Security (ARES'06)*. https://doi.org/10.1109/ares.2006.96

Juels, A. (2006). RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communications*, *24*(2), 381–394. https://doi.org/10.1109/jsac.2005.861395

Anderson, K. B., Durbin, E., & Salinger, M. A. (2008). Identity theft. *Journal of Economic Perspectives*, *22*(2), 171–192. https://doi.org/10.1257/jep.22.2.171

Lai, F., Li, D., & Hsieh, C.-T. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems*, *52*(2), 353–363. https://doi.org/10.1016/j.dss.2011.09.002

Bilge, L., Strufe, T., Balzarotti, D., & Kirda, E. (2009). All your contacts are belong to Us. *Proceedings of the 18th International Conference on World Wide Web - WWW '09*. https://doi.org/10.1145/1526709.1526784

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? *Journal of Policy Analysis and Management*, *30*(2), 256–286. https://doi.org/10.1002/pam.20567

Want, R. (2006). An introduction to RFID technology. *IEEE Pervasive Computing*, *5*(1), 25–33. https://doi.org/10.1109/mprv.2006.2

Khoo, B. (2011). RFID as an enabler of the internet of things: Issues of security and privacy. *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*. https://doi.org/10.1109/ithings/cpscom.2011.83

Hussain, A., Mkpojiogu, E. O. C., Kamal, F. M., Wahab, R. binti, & Che Meh, N. H. (2021). An instrumental assessment of touch'n go ewallet mobile app. *International Journal of Interactive Mobile Technologies (IJIM)*, *15*(06), 4. https://doi.org/10.3991/ijim.v15i06.20605

Son, I., Lee, H., Kim, G., & Kim, J. (2015). The effect of Samsung Pay on korea equity market: Using the Samsung's Domestic Supply Chain. *Advanced Science and Technology Letters*. https://doi.org/10.14257/astl.2015.114.10