Management Analysis Journal 12 (2) (2023)

http://maj.unnes.ac.id

BUILDING TRUST IN THE DIGITAL AGE: HOW HRM AND CYBERSECURITY COLLABORATE FOR EFFECTIVE STAKEHOLDER RELATIONS

Gagas Gayuh Aji[1]✉, Suko Widodo[2], Ganjar Ndaru Aji[3], Gilang Gusti Aji[4], Dian Prawitasari[5]

[1,2,3]Universitas Airlangga, Indonesia
[4]Universitas Negeri Surabaya, Indonesia
[5]Universitas Dian Nuswantoro, Indonesia

Article Information

History of article:
Accepted May 2023
Approved June 2023
Published June 2023

Keywords:
Cybersecurity, Technology Adoption, Public Relations, Customer Trust, Data Protection

Abstract

This study emphasizes the crucial role of cybersecurity and public relations in successfully adopting technology. The aim is to understand how digital technologies integrate various aspects of an organization's operations. Then, to protect customer data and manage risks, organizations need robust cybersecurity measures. At the same time, building trust and differentiation through transparent communication and addressing customer concerns is vital. This qualitative research study examines firm technology adoption in the context of cybersecurity through semi-structured interviews with a Practitioner Lecture of Information Systems. Thematic content analysis analyzes the interview data and identifies key themes and patterns. The findings provide valuable insights into the factors influencing technology adoption in cybersecurity, with efforts made to ensure a structured and rigorous approach to the analysis process. Recommendations include enhancing cybersecurity, training employees, prioritizing data privacy, maintaining ongoing public relations efforts, and collaborating with industry peers. By implementing these recommendations, organizations can navigate technology challenges, safeguard data, and cultivate a positive reputation.

✉correspondence Address:
Jl. Dharmawangsa Dalam Selatan No.28 - 30,
Airlangga, Kec. Gubeng, Surabaya, Jawa Timur 60286
E-mail: gagas.gayuh.aji@vokasi.unair.ac.id

e-ISSN 2502-1451

INTRODUCTION

The evolution of information systems in the business context has witnessed a remarkable progression from Enterprise Resource Planning (ERP) systems to the integration of Artificial Intelligence (AI) and the Internet of Things (IoT). ERP systems, introduced in the 1990s, aimed to streamline and automate various business processes, ranging from finance and human resources to supply chain management (Bar et al., 2013; Mahmood et al., 2020). These systems provided a centralized platform for data storage, transaction processing, and reporting, enabling organizations to enhance efficiency and decision-making (Laudon & Laudon, 2013; Mahmood et al., 2020).

Example of citing an article: One government action to solve this is privatization. Privatization policy in SOE was first performed in 1991 on PT Semen Gresik, Tbk. (Ministry of SOE). Several studies state that the financial performance of government companies increases after privatization (Dharwadkar et al., 2000; Gupta, 2005; Urga et al. 2007; Ochieng & Anwar, 2014). A study on the difference of performance before and after privatization in Indonesia has been performed but the result is limited to significant performance improvement in real sales (Juoro, 2002).

By reengineering and automating business processes, facilitating data sharing, and providing real-time access to updated information, ERP systems brought uniformity and consistency to the entire organization. By consolidating diverse functions under one umbrella, ERP systems streamlined operations, enhanced resource management, and promoted efficiency (Laudon & Laudon, 2013; Mahmood et al., 2020). With the ability to share data seamlessly and access real-time information, organizations could make informed decisions and respond promptly to changing business needs. ERP systems played a critical role in transforming how organizations operate, ensuring optimal utilization of resources and fostering improved productivity and performance.

The transformation from ERP systems to the integration of Artificial Intelligence (AI) and the Internet of Things (IoT) holds great potential for revolutionizing the workplace environment. The Internet of Things (IoT) is a rapidly advancing technology set to significantly improve various aspects of human life, including health, commerce, and transportation (Grammatikis et al., 2019). It encompasses an interconnected network of vehicles, physical devices, software, and electronic devices that exchange information and knowledge (Kuri & Rafi, 2020).

The IoT infrastructure relies on sensors, actuators, RFID tags, and networking technologies to create a secure and reliable platform for exchanging data and interactions between interconnected objects (Kuri & Rafi, 2020). By leveraging AI capabilities and IoT connectivity, organizations can harness the power of real-time data, automation, and intelligent decision-making to transform the workplace, enhance productivity, and unlock new opportunities for innovation and growth.

Despite the numerous benefits of Internet of Things (IoT) devices, their security has often been overlooked, primarily focusing on enhancing device capabilities rather than ensuring robust protection (Kuri & Rafi, 2020). This lack of emphasis on device security raises concerns about the vulnerability of data transmitted through the IoT network, putting user privacy at risk (Kuri & Rafi, 2020). The information shared is susceptible to being targeted, exposing personal data, and prone to hacking (Kuri & Rafi, 2020). Additionally, the IoT, like any communication network, faces various vulnerabilities and security threats (Grammatikis et al., 2019).

The extended nature of the IoT, which combines multiple technologies such as wireless sensor networks, optics networks, and mobile broadband, introduces new security challenges (Grammatikis et al., 2019). IoT objects' autonomous and automatic interaction with their environment further compounds security and privacy concerns (Grammatikis et al., 2019). Moreover, the extensive interconnections among users and objects generate vast amounts of data that can be difficult to manage securely (Grammatikis et al., 2019). These risks highlight the urgent need for robust security measures and proactive strategies to protect IoT devices and the sensitive data they handle.

Numerous studies have addressed the security challenges associated with the Internet of Things (IoT) (Kuri & Rafi, 2020; Grammatikis et al., 2019). Some studies have focused on identifying the security requirements, challenges, and threats the IoT poses (Kuri & Rafi, 2020; Grammatikis et al., 2019). For example, Suo et al. (2012), Kumar et al. (2016), Schaumont (2017), and Lin et al. (2017) have examined the overall security landscape of the IoT and its associated vulnerabilities. Additionally, researchers have explored specific areas such as IoT protocols (Granjal et al., 2015; Nguyen et al., 2015; Krej et al., 2017; Celebucki et al., 2018; Sain et al., 2017), security mechanisms and processes (Sicari et al., 2015; Zarpelo et al., 2017; Ammar et al., 2018; Ouaddah et al., 2017), and access control (Ouaddah et al., 2017).

While these studies have contributed significant efforts, the evolving nature of cyberattacks necessitates comprehensive survey papers to provide up-to-date and valuable insights (Grammatikis et al., 2019). By examining various facets of IoT security, researchers aim to develop effective solutions and countermeasures to mitigate potential risks and ensure the secure operation of IoT devices and networks.

The cyber security incident recently involving BSI highlights the complex and evolving nature of cyber threats organizations face today. Cyber attackers constantly develop sophisticated techniques to exploit vulnerabilities in organizations' systems and networks. In the case of BSI, unauthorized access and potential data breaches demonstrate the critical importance of robust security measures to protect sensitive information.

One of the main challenges firms face is the ever-increasing sophistication of cyber attacks. Attackers employ advanced techniques such as social engineering, malware, and zero-day exploits to bypass traditional security defenses. This requires organizations to continually adapt and enhance their security measures to detect and mitigate these evolving threats. Additionally, the interconnected nature of digital systems and the rapid adoption of technologies like cloud computing and the Internet of Things (IoT) introduce new attack vectors and complexities that organizations must address.

With the increasing reliance on digital technologies and the growing sophistication of cyber attacks, organizations face the challenge of protecting their systems and data from potential breaches. This paper addresses the formulation of the problem, which centers around enhancing cyber security and risk management in organizations to establish and reinforce their branding in the eyes of consumers. Organizations can effectively mitigate the potential impact of cyber-attacks by developing a conceptual framework, thus building consumer trust and confidence.

The central problem addressed in this study is how organizations can enhance their cyber security practices and risk management strategies to establish a solid organizational brand that instills a sense of security and reliability in consumers. In today's interconnected world, where consumer transactions increasingly occur in digital spaces, ensuring the protection of consumer data and maintaining a robust cyber security posture are critical. Hence, exploring and developing a conceptual framework that integrates relevant components and methodologies to enhance cyber security and risk management is necessary, thereby improving organizational branding and consumer perceptions.

LITERATURE REVIEW

Technology adoption, whether it involves implementing customer relationship management (CRM) systems or deploying emerging technologies like chatbots, often presents organizations with significant challenges and risks. Previous research has shown that CRM implementation has led to considerable dissatisfaction and low success rates (Santouridis & Tsachtani, 2015; Steel et al., 2013; Öztayşi et al., 2011). Similarly, introducing chatbots as a new technology raises concerns about how consumers perceive and utilize these automated systems (Bernazzani, 2018).

One critical aspect of successful technology adoption is the management of performance and the measurement of its outcomes. The "productivity paradox," discussed in the IT literature, explains the varied results observed in technology adoption efforts (Albadvi et al., 2007; Santhanam & Hartono, 2003; Bharadwaj, 2000). This paradox refers to the observation that introducing new technologies does not always improve productivity or performance as anticipated. It highlights the need for a deeper analysis of technology adoption performance and its measurement (Richards & Jones, 2008).

In the context of chatbots, providing consumers with a positive experience is crucial for successful implementation. Consumers expect relevant information, high system availability, personalized solutions, and seamless redirection to appropriate organizational authorities to address their queries effectively (Bernazzani, 2018). The quality dimensions of information systems, as outlined in the IS success model, play a vital role in shaping customer experience and satisfaction (Delone & McLean, 2003). Therefore, organizations must ensure that chatbots are designed and deployed to meet these quality criteria.

However, the adoption of chatbots also introduces perceived risks for consumers. As a relatively new technology, chatbots may raise concerns about privacy, security, reliability, and the potential for inaccurate or misleading information (Bernazzani, 2018). This perceived risk can influence consumers' acceptance and usage of chatbots, even if the systems are designed to meet the quality dimensions of information systems. Consequently, it is essential to consider the moderating function of perceived risk in the relationship between quality dimensions and consumer experience.

Furthermore, the impact of using technology, particularly artificial intelligence (AI), on consumer decision-making processes and firm-consumer relationships requires further exploration (Poushneh & Vasquez-Parraga, 2017; Dawar & Bendle, 2018). AI-powered chatbots have the potential to enhance convenience for consumers and transform how organizations interact with their customers. However, understanding how AI influences consumer behaviors and expectations in the context of technology adoption is a complex endeavor.

Achieving the best consumer/user experience and ensuring robust cyber security measures are paramount in technology adoption, including implementing CRM systems and deploying chatbots. Furthermore, with the emergence of new collaborative technologies, customers interact continuously with organizations during every stage of the relationship spectrum, leading to deeper collaboration and improved mutual understanding of needs (Payne et al., 2008; Ballantyne, 2004).

To deliver the best consumer/user experience, organizations must embrace collaborative technologies enabling ongoing customer interactions. This continuous engagement allows a deeper understanding of customer needs, preferences, and expectations. Organizations can gather valuable data and insights by leveraging CRM systems and chatbots, enabling personalized and targeted customer interactions (Payne et al., 2008).

Implementing collaborative technologies also facilitates a more seamless and integrated customer experience. Organizations can use CRM systems to capture and store customer information, interactions, and purchase history. Chatbots can leverage this data to provide personalized recommendations, resolve customer queries efficiently, and offer tailored solutions (Ballantyne, 2004).

Moreover, collaboration through these technologies enhances the mutual understanding of needs between organizations and customers. Organizations can proactively gather customer feedback, suggestions, and insights to improve products, services, and overall customer experience (Payne et al., 2008). By actively involving customers in value co-creation, organizations can foster a sense of ownership and loyalty, resulting in long-term customer relationships.

While pursuing the best consumer/user experience, organizations must recognize the importance of robust cyber security measures. Collaborative technologies inherently involve the exchange of sensitive data and personal information. Therefore, organizations must implement stringent security protocols to safeguard customer data and protect against cyber threats (Dawar & Bendle, 2018).

A robust cyber security framework includes encryption, secure data storage, user authentication, and proactive monitoring of potential vulnerabilities. Regular audits and updates to security protocols are crucial to staying ahead of emerging cyber threats and ensuring ongoing protection for organizations and customers (Dawar & Bendle, 2018).

Achieving the best consumer/user experience requires the integration of collaborative technologies that enable continuous interactions and mutual understanding of needs. CRM systems and chatbots capture customer insights, provide personalized experiences, and foster collaboration throughout the customer relationship spectrum. However, organizations must prioritize robust cybersecurity measures to protect customer data and mitigate risks associated with collaborative technologies. By striking the right balance between collaboration, customer experience, and cyber security, organizations can build strong relationships, drive customer loyalty, and safeguard their reputation in the digital landscape.

METHOD

This study employs a qualitative research approach to investigate the phenomenon of firm technology adoption. Qualitative research methodology is deemed suitable for studying technology adoption and the customer experience in cybersecurity when existing research studies are scarce (Alshamaila et al., 2013; Kwon et al., 2014; Schultze and Avital, 2011). Semi-structured interviews were conducted with Practitioner Lecture of Information System to explore cybersecurity in organizations context. The utilization of multiple sources of information is recommended to enhance the reliability of the findings (Fielding, 2012; Franklin et al., 2010; Patton, 1999).

Thematic content analysis was employed as the method for analyzing the primary data. Thematic content analysis has been previously used in information studies research to identify determinants of technology adoption (Alshamaila et al., 2013; Nasir, 2005; Sun et al., 2018). The findings from the thematic content analysis of the semi-structured interview texts were then deduced with the theoretical framework. Thematic content analysis was chosen as the preferred research method for this study due to the relatively large sample size and the involvement of two researchers in the data analysis process (Braun and Clarke, 2006). This method provides a more structured approach to analyzing data and facilitates clear and organized data analysis reporting (King, 2004).

It is essential to acknowledge that thematic content analysis has limitations in terms of rigor and potential inconsistencies compared to other qualitative research methods, such as grounded theory, ethnography, and phenomenology (Nowell et al., 2017). However, in this study, efforts were made to follow a structured approach to thematic analysis, including familiarizing ourselves with the data, generating initial codes, discovering and reviewing themes collaboratively, categorizing and naming pieces, and producing the final report. Direct quotes from the respondents were included in the report-writing process as a vital component to bring depth and richness to the findings of this study (King, 2004).

RESULT AND DISCUSSION

Perspective	Findings
Public Relations	Transparent communication and open disclosure of cybersecurity incidents are essential for maintaining customer trust
Human Resource Management	Employee training on cybersecurity awareness is crucial for developing a cybersecurity-focused workforce (Axeland et al., 2021; Cornelius et al., 2022). Collaborating with IT
Management	Aligning marketing, public relations, and human resource management ensures a holistic approach to enhancing cybersecurity practices.

The findings of this study emphasize the critical importance for organizations to enhance cybersecurity measures and build strong public relations. Organizations face heightened cybersecurity risks in today's digital landscape, where technology adoption is prevalent, and customer interactions are increasingly conducted online. Protecting sensitive information and maintaining customer data's privacy and integrity is paramount to establishing and maintaining trust with customers.

Cybersecurity breaches can have severe consequences, including financial losses, reputational damage, and loss of customer trust (Axeland et al., 2021; Akpan et al., 2022; Cornelius et al., 2022). Therefore, organizations must invest in robust cybersecurity infrastructure, implement stringent security protocols, and stay updated with the latest security measures and technologies. Organizations can mitigate the risks associated with technology adoption by prioritizing cybersecurity, safeguarding customer data, and protecting their systems and operations (Teymourlouei & Jackson, 2021).

The findings of this study also highlight the critical role of marketing and public relations in the successful adoption of technology and cybersecurity. In today's digital landscape, organizations must prioritize transparent communication and data handling practices, especially after cybersecurity incidents like data leaks. Maintaining open and honest communication with customers is essential to building trust and mitigating the negative impact of such incidents on the organization's reputation (Axeland et al., 2021; Cornelius et al., 2022).

Marketing management plays a significant role in technology adoption by considering the impact of cybersecurity risks on marketing strategies and customer perceptions. Organizations must prioritize cybersecurity measures to protect customer data and maintain brand reputation. Transparent communication about data privacy and security practices is crucial to reassure customers and maintain their trust (Rivero & Theodore, 2014). By integrating cybersecurity considerations into marketing strategies, organizations can build a positive image, differentiate themselves from competitors, and attract and retain customers (Axeland et al., 2021; Cornelius et al., 2022).

Human resource management is critical in addressing technology adoption challenges and enhancing cybersecurity practices. Developing a cybersecurity-focused workforce requires employee training on cybersecurity awareness and best practices. Collaborating with IT departments ensures the recruitment and retention of skilled professionals who can effectively manage technology risks and safeguard organizational systems and data. By investing in employee training and fostering a culture of cybersecurity awareness, organizations can reduce the likelihood of breaches and protect sensitive information (Axeland et al., 2021; Cornelius et al., 2022).

The interconnectedness of marketing, public relations, marketing management, and human resource management is evident in the context of technology adoption and cybersecurity. Effective marketing and public relations practices build trust and credibility, while marketing management integrates cybersecurity considerations into strategies to protect brand reputation. Human resource management plays a crucial role in training and developing a cybersecurity-focused workforce, promoting a culture of awareness and accountability (Rivero & Theodore, 2014).

In conclusion, organizations must prioritize transparent communication, robust cybersecurity measures, and employee training to navigate technology adoption challenges successfully. Organizations can mitigate risks, build customer trust, and enhance their cybersecurity posture by aligning marketing, public relations, marketing management, and human resource management. This integrated approach contributes to the organization's long-term success in a digital business environment (Axeland et al., 2021; Cornelius et al., 2022; Rivero & Theodore, 2014).

CONCLUSSION AND RECOMMENDATION

This study emphasizes the critical significance of enhancing cybersecurity measures and building solid public relations in technology adoption. Organizations must prioritize cybersecurity to protect customer data and mitigate risks in the digital landscape. Simultaneously, effective public relations practices are crucial for establishing trust and maintaining positive customer relationships. By integrating robust cybersecurity measures, providing employee training, fostering a culture of data privacy, engaging in continuous public relations efforts, and collaborating with industry partners, organizations can navigate technology challenges, safeguard data, and cultivate a positive reputation.

Recent events, such as the BSI data breach (Muthiariny, 2023), highlight the need for transparent customer communication. Organizations should prioritize transparent communication to regain trust and address potential negative impacts. Collaboration with industry partners and experts can provide valuable insights into addressing cybersecurity challenges and strengthening data protection measures (Muthiariny, 2023). Organizations can enhance their resilience, protect customer data, and restore confidence in their technology adoption processes by implementing the recommended cybersecurity and public relations strategies.

In conclusion, this study underscores the importance of enhancing cybersecurity measures and building solid public relations in technology adoption. Organizations must prioritize cybersecurity, invest in employee training, foster a culture of data privacy, engage in continuous public relations efforts, and collaborate with industry partners. By doing so, organizations can navigate technology challenges, protect customer data, and cultivate a positive reputation in the digital era. Recent incidents, such as the BSI data breach, emphasize the need for transparent communication and collaboration to address cybersecurity risks effectively. By implementing the recommended strategies, organizations can enhance their resilience and restore customer confidence in their technology adoption processes.

REFERENCES

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity challenges in the maritime sector. Network, 2(1), 123-138.

Ammar, M., Russello, G., & Crispo, B. (2018). Internet of things: A survey on the security of IoT frameworks. Journal of Information Security and Applications, 38, 8-27.

Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015). Internet of things: Security vulnerabilities and challenges. 2015 IEEE Symposium on Computers and Communication (ISCC), 180-187.

Axeland, Å., Hagfeldt, H., Carlsson, M., Sergel, L. L., & Butun, I. (2021). Implications of cybersecurity breaches in LPWANs. In Decision Support Systems and Industrial IoT in Smart Grid, Factories, and Cities (pp. 1-18). IGI Global.

Boiko, A., Shendryk, V., & Boiko, O. (2019). Information systems for supply chain management: Uncertainties, risks and cybersecurity. Procedia Computer Science, 149, 65-70.

Celebucki, D., Lin, M. A., & Graham, S. (2018). A security evaluation of popular internet of things protocols for manufacturers. 2018 IEEE International Conference on Consumer Electronics (ICCE), 1-6.

Cornelius, F. P., van Rensburg, S. K. J., & Kader, S. (2022). The value of criminological theories in explaining cybersecurity in South African smart cities. International Annals of Criminology, 60(2), 220-240.

Dubey, N. K., & Sangle, P. (2019). Customer perception of CRM implementation in banking context: Scale development and validation. Journal of Advances in Management Research, 16(1), 38-63.

Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the internet of things: A survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials, 17(3), 1294-1312.

Grammatikis, P. I. R., Sarigiannidis, P. G., & Moscholios, I. D. (2019). Securing the Internet of Things: Challenges, threats and solutions. Internet of Things, 5, 41-70.

H. Suo, J. Wan, C. Zou, J. Liu. (2012). Security in the internet of things: A review. 2012 International Conference on Computer Science and Electronics Engineering, Vol. 3, 648–651.

Kamariotou, M., & Kitsios, F. (2019). Information systems planning and success in SMEs: Strategizing for IS. In Business Information Systems: 22nd International Conference, BIS 2019, Seville, Spain, June 26–28, 2019, Proceedings, Part I 22 (pp. 397-406). Springer International Publishing.

Kumar, A., & Krishnamoorthy, B. (2020). Business analytics adoption in firms: A qualitative study elaborating TOE framework in India. International Journal of Global Business and Competitiveness, 15(2), 80-93.

Kuri, J. L., & Rafi, M. (2020). Securing data in Internet of Things (IoT) using cryptography and steganography techniques. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 8(7), 1933. Retrieved from www.ijraset.com.

Laudon, C. K., & Laudon, P. J. (2013). Essentials of management information systems. Pearson Education, Inc.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things Journal, 4(5), 1125-1142.

Leloglu, E. (2017). A review of security concerns in internet of things. Journal of Computer and Communications, 5(1), 121-136.

Mosenia, A., & Jha, N. K. (2017). A comprehensive study of security of internet-of-things. IEEE Transactions on Emerging Topics in Computing, 5(4), 586-602.

Muthiariny, D. E. (2023, May 26). BSI Admits Massive Money Withdrawals Post Service Disruptions. Tempo. https://en.tempo.co/read/1730272/bsi-admits-massive-money-withdrawals-post-service-disruptions

Nguyen, K. T., Laurent, M., & Oualha, N. (2015). Survey on secure communication protocols for the internet of things. Ad Hoc Networks, 32, 17-31.

Ouaddah, A., Mousannif, H., Elkalam, A. A., & Ouahman, A. A. (2017). Access control in the internet of things: Big challenges and new opportunities. Computer Networks, 112, 237-262.

Qu, Y., Ming, X., Ni, Y., Li, X., Liu, Z., Zhang, X., & Xie, L. (2019). An integrated framework of enterprise information systems in smart manufacturing system via business process reengineering. Proceedings of the Institution of Mechanical Engineers, Part B: Journal of

Engineering Manufacture, 233(11), 2210-2224.

Rivero, O. (2014). The importance of public relations in corporate sustainability. Global Journal of Management and Business Research, 14(B4), 21-23.

Sain, M., Kang, Y. J., & Lee, H. J. (2017). Survey on security in internet of things: State of the art and challenges. 2017 19th International Conference on Advanced Communication Technology (ICACT), 699-704.

Schaumont, P. (2017). Security in the internet of things: A challenge of scale. Design, Automation Test in Europe Conference Exhibition (DATE), 674-679.

Sicari, S., Rizzardi, A., Grieco, L., & Coen-Porisini, A. (2015). Security, privacy and trust in internet of things: The road ahead. Computer Networks, 76, 146-164.

Teymourlouei, H., & Jackson, L. (2021). Dark Data: Managing Cybersecurity Challenges and Generating Benefits. In Advances in Parallel & Distributed Processing, and Applications: Proceedings from PDPTA'20, CSC'20, MSV'20, and GCC'20 (pp. 91-104). Springer International Publishing.

Trivedi, J. (2019). Examining the customer experience of using banking chatbots and its impact on brand love: The moderating role of perceived risk. Journal of Internet Commerce, 18(1), 91-111.

Zarpelo, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in internet of things. Journal of Network and Computer Applications, 84, 25-37.