Establishing an Integrated Push Notification System with Information Security Mechanism

Hsin-Te Wu(✉)

Department of Computer Science and Information Engineering, National Ilan University, Yilan, Taiwan
hsinte@niu.edu.tw

Abstract. Today, many enterprises and governmental units utilize push technology to deliver messages. To enterprises, the system can announce company policies rapidly; to clients, it can distribute new events or promotions. There are many approaches to convey messages, such as emails and text and LINE messages; however, it requires a method to protect client information and avoid hackers or data theft by internal staff. The paper aims to develop a push notification system similar to a set-top box, and the system includes below features. 1. Establishing a set-top push system and server for firms to set login information. 2. Creating a function module for the operator to select suitable marketing models. 3. The integrated push notification system offers enterprises to send messages through emails, texts, and LINE application. 4. Through creating groups and user-friendly interfaces, operators could easily send push notices to various groups. 5. Build a hierarchical message authentication mechanism; the hierarchical method enables operators to review message content and ensure the correctness. 6. Develop personal information encryption and an Internet security mechanism to confirm the source, completeness, and authentication. 7. The personal information encryption protects the system from internal staff to export critical data. Clients will only need to rent the modules they need, and the supplier is in charge of providing the server and set-top push system, which will help to universalize the product.

Keywords: Natural language processing · Push technology · Network security · Personal information protection · Internet of Things

1 Introduction

With the development and application of mobile devices and mobile networks, information has become increasingly transparent. In the past, many marketers used flyers or letters for product promotion or event marketing information transmission. With the advent of virtual and real integration and the advent of the mobile era, many promotional activities are based on social Group software or SMS messaging allows customers to instantly grasp the latest promotions and make purchases through mobile phones. However, in the past, the cost of using SMS to push and broadcast was relatively high. For telecommunications manufacturers, a corporate newsletter cost 0.8 yuan. Small-scale e-commerce companies send large numbers of newsletters are a big burden, so

T. Nakano (Ed.): BICT 2021, LNICST 403, pp. 26–32, 2021.
https://doi.org/10.1007/978-3-030-92163-7_3

many companies nowadays use social software as the main message to push and broadcast. At present, many push broadcasts combine AI (Artificial Intelligence) for semantic analysis, and build dialog robots to understand customer needs based on client semantic analysis. The robots will answer customer questions according to needs, and collect customer-related questions for analysis, and understand the general customer's product. The frequently asked questions are improved, and the message push and broadcast combined with the dialogue robot effectively achieve the effect of 24-h customer service.

Nowadays, most people are accustomed to using social software for message transmission or information acquisition. Therefore, this paper's push broadcast system is added to Line's social software, and there is no upper limit for push messages. This paper mainly uses set-top boxes and module rentals. Therefore, price parity can help Taiwan's small and medium-sized enterprises or small e-commerce use. Message transmission is an important part of marketing. Therefore, companies can use this system to transmit the latest information to customers, and companies can classify customers and transmit marketing information according to customer groups. Due to the shortage of manpower for small and medium-sized enterprises, this system introduces artificial intelligence to provide customer service. In addition, this plan will classify customer problems one by one to help the company improve its products. At present, the security of customer data is very important, so this plan also introduces information security Mechanism to ensure the safety of customers' personal information, and internal personnel cannot obtain customer plaintext data from the server.

The methods proposed in this paper are mainly as follows: 1. Build an integrated push broadcast set-top box, and the equipment can be placed in the computer room for environmental monitoring. Each enterprise can set the set-top box account secret and organize the personnel account secret to ensure the data. Security, 2. In a functional modular way, companies can choose suitable functions. This plan uses the Internet of Things to build a set-top box to build a small exclusive business service station, and the data between companies will not circulate to ensure information. Security, 3. Build an integrated message push system. The message push methods include telephone, E-mail, SMS and Line, so that companies can choose the message push method, allowing the operator to push messages to SMS, In mail and Line, when some industries need urgent notification, they need to use the phone to notify relevant personnel to return to the company, or when the computer room environment is abnormal, they also need to notify. 4. Establish groups and simple UI interfaces to facilitate the group broadcast by operators. 5. Establish a hierarchical message content verification mechanism, through hierarchical personnel to view the message content, to ensure the correctness of the content, 6. Establish a network security mechanism to ensure the source, integrity and identity verification of the sent message, 7. Build a personal The data protection encryption mechanism prevents internal personnel from exporting customer personal data. The product customers of this plan only need to rent the required functions, and the server and set-top box are the responsibility of the manufacturer, which helps to popularize the product.

2 Related Works

In the literature [1], it is mainly mentioned that the Internet of Things is mainly based on real-time systems. Therefore, the overall system design must be lightweight to achieve real-timeness, and other systems need to add security mechanisms to ensure data security. . In the literature [2], it is mainly mentioned that the data of the Internet of Things is too large, so the Internet of Things needs to combine cloud computing or fog computing to store the data in a spatially penetrating storage before data processing or analysis can be performed. In the literature [3], VR-IOT is mainly proposed, in which IoT information transmission needs to rely on XML for mutual transmission, and MQTT is used for IoT device control. , The paper method information is sent to the server for backup. When the set-top box is damaged, the data can be imported from the server back to the new set-top box. In addition, when the set-top box module needs to be updated, the plan. If the XMPP system is installed, the module can be updated through commands, which can achieve the effect of system optimization.

In the literature [4], ID-based is mainly used for distributed data verification. As long as any party obtains the ID of the other party and then uses bilinear pairing to verify the legitimacy, the integrity and authentication of the data can be determined. He He 2015 mainly uses ID-based privacy and data security mechanisms for building ad hoc networks for vehicles. Through the ID-based mechanism, the anonymous ID of the vehicle can be effectively established, and when the vehicle commits a crime, the real ID of the vehicle can be passed. In the literature [5], bilinear pairing is mainly used to create data signatures, which can effectively verify the correctness of data. In the literature [6], bilinear pairing is mainly used to establish a security mechanism without public/private key authentication. Here, the time consumed by the public/private key authentication can be overcome and complete security can be provided. And personal asset protection.

3 The Proposed Scheme

3.1 Systme Model

The schematic diagram of the project system is shown in Fig. 1. The project system is mainly divided into a set-top box and a server side. The set-top box is mainly used as a small server by the development version of the Internet of Things, in which the set-top box can be connected to a sensor , Such as: temperature and humidity, flame sensors, etc., can also be connected to monitoring equipment to monitor the environment of the computer room, in addition, the set-top box can construct a small database for data storage, and the database has information security encryption to avoid exposure when data is stolen Customer's real data. The push broadcast system mainly has telephone, mail, SMS and line message communication functions. The set-top box has a simple network management protocol (SNMP) function. When the computer room environment is abnormal, the telephone will be activated to notify the network administrator. When there is an abnormality in the plant, plant personnel can notify the engineer to return to the plant through the push broadcast system. The line push broadcast system of this project mainly uses the Line ID left by the customer to join, and uses IFTTT

(If this, then that) to perform Message transmission. On the server side, there are mainly modules and software updates, databases, and XMPP platforms. Business owners can securely connect to the server side selection module through a set-top box. The server side will record which modules the enterprise uses. When new software needs to be updated, the set-top box can be notified of the update time through the XMPP platform. The owner can choose the time to update the software. The set-top box will actively download the latest module software from the server, and the data in the set-top box will be updated. Encrypted and backed up to the database regularly to avoid data loss due to damage to the set-top box.

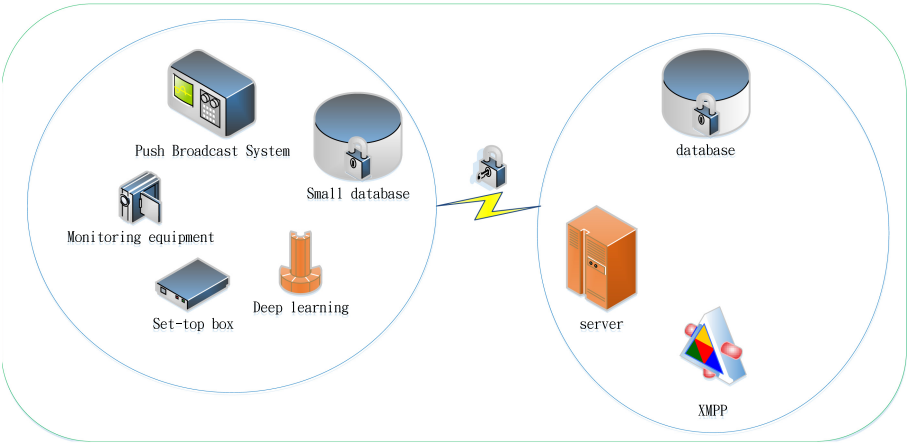

Fig. 1. XMPP system platform

3.2 Cybersecurity Mechanism Establishment

This article mainly uses Bilinear Pairings to construct an overall network security mechanism. Assuming TA is the server side, first calculate the safety factors such as the public key and Private key of the TA and the set-top box ($I_1 \sim I_n$). The calculation is as follows:

1. TA selects $c \in Z_q^*$ as the secret key, r is the public value.
2. The ID of TA is ID_{TA}, where public key is $\mathcal{PK}_{ID_{TA}} = ID_{TA} \cdot P$, and private key is $\mathcal{PR}_{ID_{TA}} = r^c \cdot ID_{TA} \cdot P$.
3. The public value of TA is $\mathcal{PU}_{ID_{TA}} = r^{\frac{1}{c}} \cdot P$.

Next, calculate the public key and private key of $I_1 \sim I_n$, which are calculated as follows:

1. The public key of I_n is $\mathcal{PK}_{ID_{I_n}} = ID_{I_n} \cdot P$.
2. The private key of I_n is $\mathcal{PR}_{ID_{I_n}} = r^c \cdot ID_{I_n} \cdot P$.

The public Key and private key of $I_1 \sim I_n$ above are the preset passwords of the set-top box. Among them ID_{I_1} is the name of the set-top box, and the company needs to change the private key when connecting for the first time.

3.3 Data Backup Mechanism

The machine-top box of this project transfers customer data and related data to the database. First, I_1 will use its own public key to encrypt. Reuse with TA $\mathcal{SK}'_{ID_{I_1} \leftrightarrow TA}$ encrypt the data and send it to TA. Calculated as $\mathcal{SK}'_{ID_{I_1} \leftrightarrow TA}\left(\mathcal{PK}_{ID_{I_1}}(M) \,||\, H\left(\mathcal{PK}_{ID_{I_1}}(M)\right)\right)||ID_{I_1}$. When the TA receives the ciphertext, it uses the common session key to decrypt it, and then verifies the integrity of the message. The TA uses hash technology to calculate $\mathcal{PK}_{ID_{I_1}}(M)$. If it is the $H\left(\mathcal{PK}_{ID_{I_1}}(M)\right)$ same, it means that the message has not been tampered with. Then the TA will use its own Public Key to encrypt it and store it in the database. When the insider steals the information, the real data M cannot be known, even if the insider steals the TA's privacy key is decrypted, but it cannot be decrypted $\mathcal{PK}_{ID_{I_1}}(M)$.

3.4 XMPP Platform Software Update Mechanism

The server and the set-top box can be securely connected through $SK\left(\mathcal{SK}'_{ID_{I_1} \leftrightarrow TA}\right)$, and the download module from the XMPP server-side can be subscribed to the set-top box. The XMPP server can record the modules subscribed to by each set-top box, and is used to calculate the amount that the company needs to pay. When the XMPP server has a module to update the software, XMPP will issue a command to the IoT development board to notify the company of the update. The upper box will request the update time after receiving the instruction. At this time, the company must set the update time. If it is not set, it will update according to the preset time.

4 Experimental Result

The XMPP server of this project can generate reports, and can also control the related sensor equipment and related modules of the set-top box through commands, which will help the system to automate the process. 1. The system can confirm whether the enterprise subscription has paid for it, if there is a system then use the command to open the function, 2. The system can automatically determine which users need to update the software, and send out notifications by itself, as shown in Fig. 2 for the XMPP system platform.

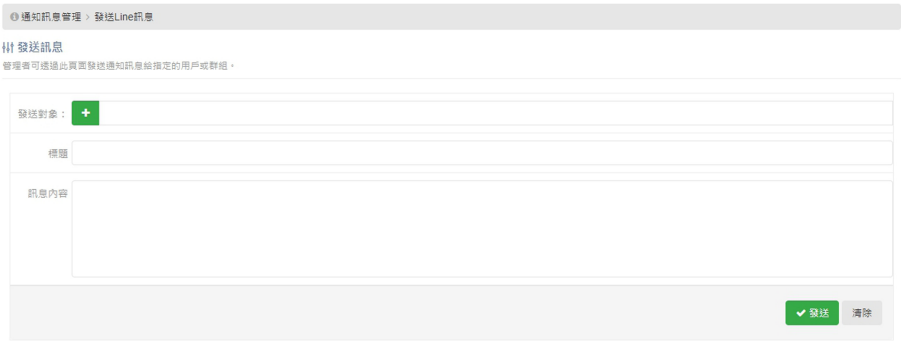

Fig. 2. XMPP system platform

5 Conclusion

Many companies develop systems that are bought out or need to build hardware and software equipment. In addition, these systems need to be installed in servers. Therefore, the need for enterprises to set up servers is a burden for enterprises. The systems proposed in this project are mainly integrated push broadcasts. The system, combined with telephone, SMS, mail and Line, allows companies to choose the way of promotion. This plan also combines with an environmental monitoring system to help companies monitor the computer room or working environment. This plan uses the Internet of Things to increase the utilization rate of the enterprise. The set-top box version is built so that companies can use the set-top box to connect to the network and use it directly, reducing the incompatibility of the company for information operations. This plan adds an information security mechanism, and all customer data in the set-top box is encrypted. When internal or external personnel steal information, they cannot decrypt the data to achieve the security of customer data. The server built by this system manufacturer mainly provides data backup, module download and software update. Data backup is encrypted, so even if the server is If the device is stolen by insiders, the plaintext of the information cannot be obtained.

Acknowledgement. The authors would like to thank the anonymous reviewers for their valuable comments and suggestions on the paper. This work was supported in part by the Ministry of Science and Technology of Taiwan, R.O.C., under Contracts MOST 109-2622-E-197-012.

References

1. Condry, M.W., Nelson, C.B.: Using smart edge IoT devices for safer, rapid response with industry IoT control operations. Proc. IEEE **104**(5), 938–946 (2016)
2. Metzger, F., Hoßfeld, T., Bauer, A., Kounev, S., Heegaard, P.E.: Modeling of aggregated IoT traffic and its application to an IoT cloud. In: Proc. IEEE **107**(4), 679–694 (2019)
3. Simiscuka, A.A., Markande, T.M., Muntean, G.-M.: Real-virtual world device synchronization in a cloud-enabled social virtual reality iot network. IEEE Access **7**, 106588–106599 (2019)

4. Wang, H.: Identity based distributed provable data possession in multicloud storage. IEEE Trans. Serv. Comput. **8**(2), 328–340 (2015)
5. Tsai, J.-L.: A new efficient certificateless short signature scheme using bilinear pairings. IEEE Syst. J. **11**(4), 2395–2402 (2017)
6. Du, H., Du, H., Wen, Q.: A provably-secure outsourced revocable certificateless signature scheme without bilinear pairings. IEEE Access **6**, 73 846–73 855 (2018)