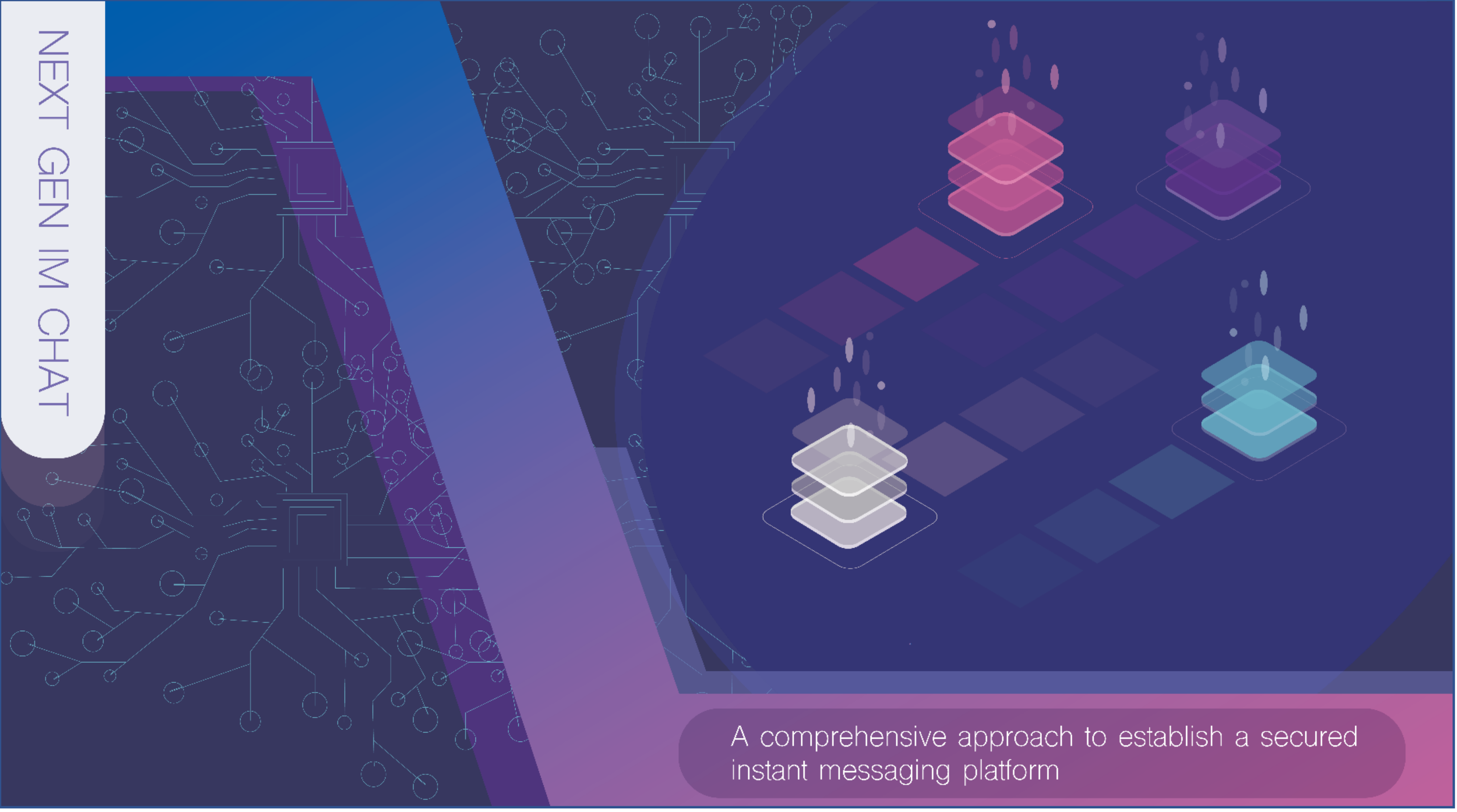


A comprehensive approach to establish a secured instant messaging platform

Privacy Outweighs Money

Who is the targeted user

Any enterprise who desired a private and secure communication within the organization may refer to this document to understand the future technology of network and information security which used privacy and security as the core philosophy to develop a custom designed encrypted communications tool.

BEYOND SECURITY LINKDOOD

Table of Content

Introduction

In this modern era, technology has enhanced privacy and information security while it also means by offering more accessible path to access the information. Things such as online transaction, messaging application and any technology which utilized a third party/public server could expose new and endangered threat to data privacy. Many enterprises make use of internet for online meeting, cloud storage for storing theirs files or even sharing private confidential information across the internet without they even realize that the information could be exposed by third party.

Due to this vulnerability, data encryption is needed to provide the data information confidential to prevent unwanted interception from unauthorized user or it may force enterprise into unwanted hazard in the middle of security and operation.

Chat on Social Media

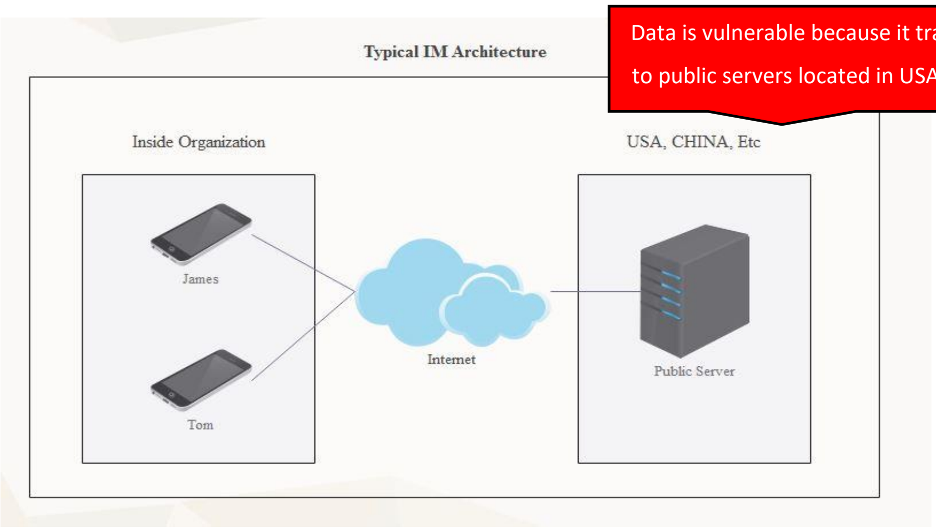
According to statistics, 90% of the world's data has been generated in the past two years. Mobile Internet, traditional Internet, and social networks are generating more and more data. Facebook processes 25TB of data per day, Twitter processes 7TB of data per day, 30TB+ Internet logs and 100TB+ signaling data every day and WhatsApp users sent 65 billion messages per day.

Some note-able key points in the report:

- **Data Leakage:** User data are being exposed to publicity across social media APP.
- **No Data Privacy:** User private confidential data/documents are disclosed to public server while offering anonymous user an illegal access to it.
- **Data Analyzed for Advertisement:** User browsing activities are being traced and the data are sold to third party advertiser to promote advertisement based on personal data analysis without user consent.

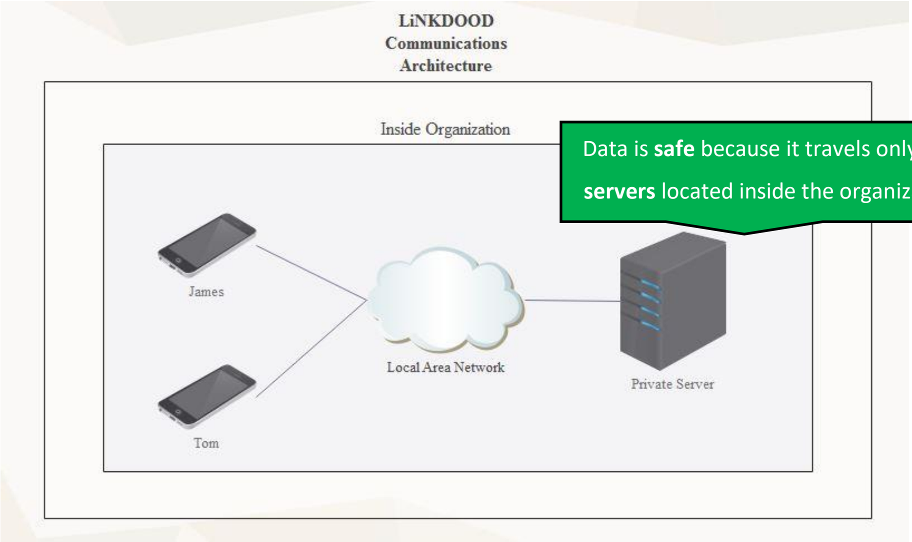
Imagine most of the existing organizations are utilizing third party social media APP for daily work meeting to communicate with each other and share confidential files through a public internet. Public online environments are not always safe and it could potential lead to data eavesdropping or interception from unwanted user. This paper purpose is to identify new threat and create a method to achieve a secured end-to-end communication.

Communication Architecture



Data is vulnerable because it travels over the Internet to public servers located in USA, China and etc.

Figure 1



Data is **safe** because it travels only in the LAN to **private servers** located inside the organization’s premise.

Figure 2

Figure 1 and Figure 2 show the comparison between Typical IM Architecture and LiNKDOOD Communication Architecture. To address the information security threat in a typical IM architecture environment, it is important to understand the current internet environment situation where end user sent their data into it. Data is vulnerable because it travels over the Internet to public servers located in USA, China and etc. On the other hand, LiNKDOOD Communications Architecture utilized a private server where data is safe because it travels only in the LAN to private servers located inside the organization’s premise. With its custom designed encryption tools, it could narrow down a large number of data security threat within the organization and prevent from being exposed to a crossfire anonymous attack. Thus, highly reduced the risk of data interception and enhanced data security.

The Next Gen of Secured Communication

LiNKDOOD brings the future of communication systems. With privacy and security at the core of philosophy, LiNKDOOD brings a cross-device, omnidirectional secured communication platform. Based on the principal of providing secured communication, it used private servers, multiple level encryption technology to protect users’ privacy. It is supported by Android, iOS, Windows and MacOS, providing multilevel services like security cooperation, collaborative office, task management, voice/video conferences, Enterprise resources planning, application development and convergence promotion which meet users’ requirement from different industries.

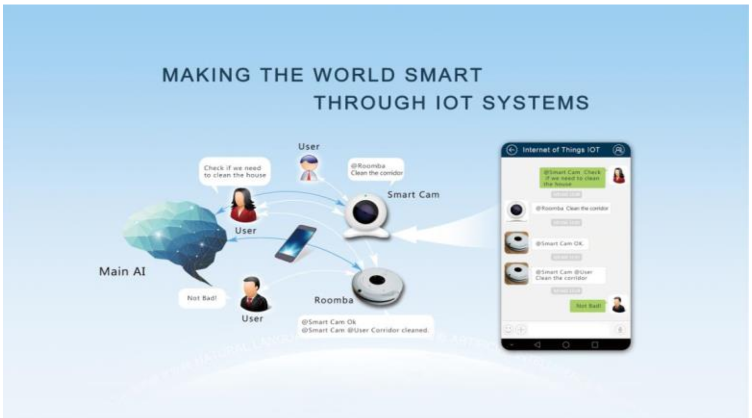

MAKING THE WORLD SMART
THROUGH IOT SYSTEMS
User
Check if we need to clean the house
@Roomba Clean the corridor
Smart Cam
User
Main AI
Not Bad!
User
Roomba
@Smart Cam Ok
@Smart Cam @User Corridor cleaned.
Internet of Things IOT
@Smart Cam Check if we need to clean the house
@Roomba Clean the corridor
@Smart Cam OK
@Smart Cam @User Clean the corridor
Not Bad!

Figure 3

LiNKDOOD provides a platform where smart devices can connect together into a network known as Internet of Things (IoT). This IoT allows devices to communicate with each other, coordinate their action in order to perform specific task in more efficient and productive way.

LiNKDOOD secured communication platform has full IM functions such as messaging, group chat, voice/video chat, file transmission, and so on. Furthermore, it also provides large-scale applications essentially for Check-In, cloud storage, email and many more! Other special functions are described as below:

- **Delay Message:** Pre-set the message delivery time to be sent. Manage your own message schedule today.
- **Analytic:** provides users with the latest articles/news and gather survey data to allow a more customized result to suit their individual likes.
- **Task:** A task assignment tool which allows user to deliver tasks under chat mode, as well as monitoring member progress.
- **Eraser:** Completely clear any conservation history with user consent, leaving no trace on both client and server. In group chat case, only the administrator has the permission to use the eraser.
- **Organization:** Create and form multi-level organization within an enterprise. This allow strategy management to control different user from different organization.
- **Hidden Contact:** Hide user private contact easily with a password gesture. Different gesture creates a different group of hidden contacts.
- **Encrypted Message**: conceal user chat message with a passcode. Only users which have the same passcode are able to view the message.
- **Burnchat:** Send a disposable message among users. The message will auto delete itself after a period of time and user device screenshot are restricted. If any user tried to screenshot the message content, it will deliver a message receipt to alert the sender.
- **Multi-Server:** Manage multiple server within an APP, different server for different business.

LiNKDOOD Platform Architecture

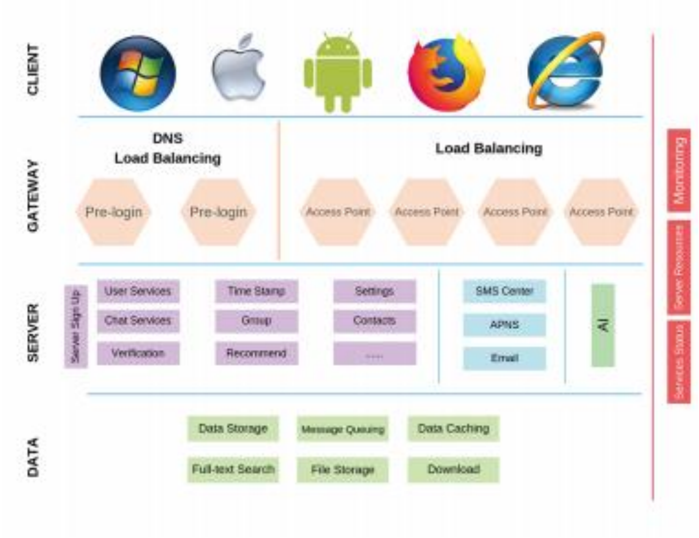


Figure 4

LiNKDOOD Secured Communication Platform adopts an open structure to create extensible and compartmentalized platforms. Each structure is briefly explained as below:

- **Client**

Support a number of platforms including Windows, MacOS. Mobile ends including iOS and Android. Browsers including Chrome, Firefox, IE etc.

- **Gateway**

Provides load balancing access to pre-login services, access point server address information, server configuration and logic upgrade; it also provides multiple access points, which call upon different services from server level to meet the demands of client end.

- **Server**

The services are divided into service cells categorized by the type of service. Each cell provides an API in order to handle requests from the client-end. The Push and Send center handles all operations related to APNS, SMS and Email.

- **Data**

LiNKDOOD provides services such as data storage, message queuing, data caching, message searching, file storage and download. Artificial intelligence transforming machine into a human-alike, achieving physical control of devices thru message conversation.

- **Monitor**

Monitors running server operation (CPU, memory, hard-drives, network etc); which monitor the server status.

Open Coordination Platform

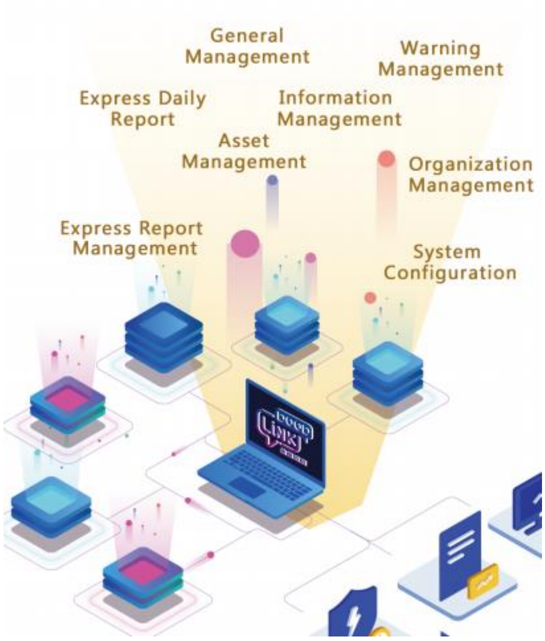


Figure 5

LiNKDOOD provides their developers with a complete SDK development kit where developers are able to connect to their existing system to create their own APP easily with secure communication capabilities. Moreover, LiNKDOOD allows its users to use various different third-party applications, covering a wide range of function abilities. The in-built quick development platform can be constructed for enterprises business applications while supporting customization of more than 100 modules for constructing environment of visual business applications.

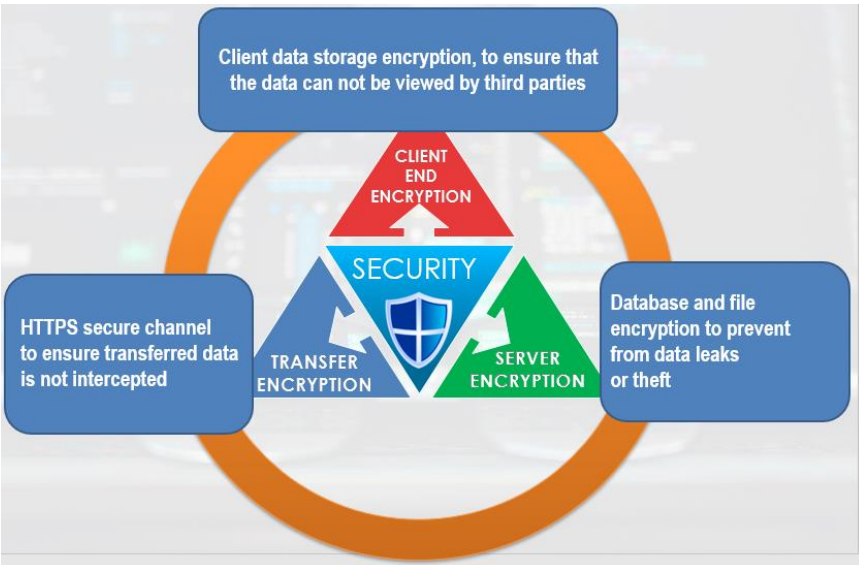
Private Data Protection

User's private data on how they are protected in LiNKDOOD Platform Architecture are explained as below:

- **Controllable Private Server**

For purpose of work communication, enterprise users without doubt will utilize a controllable server to ensure the security. LiNKDOOD secured communication platform can be deployed on both private and cloud servers, applicable for different scales from ten to hundred millions of users. With LiNKDOOD, Users control their own data.

- **Data Encrypted Multi-Dimensional Protection**


Client data storage encryption, to ensure that the data can not be viewed by third parties

HTTPS secure channel to ensure transferred data is not intercepted

Database and file encryption to prevent from data leaks or theft

Figure 6

From access, management and storage of their data, LiNKDOOD uses the privacy protected technology such as identity authentication, access control, triple end encryption, omnidirectional audit, security classification management, channel encryption. Channel integrity reinforcement, data encryption and server security enhancement are used to ensure data security and prevent data leaks.

- **Chip Customization Support**

The platform can be adapted to operate on 100% customized chips, supporting operating systems like Kylin, NeOkylin and NFS, CUP like Loongson, Zhaoxin and Phutium, mobile terminal like Lenovo, Tsinghua, Tongfang, TD and Syber, database like DM, KingbaseES and Kunlun. It also supports encryption algorithms released by State Cryptographic Administration.

LiNKDOOD Encryption Characterization

LiNKDOOD provides an end-to-end encryption of messages between terminals for secure instant messaging. At the beginning of the session, key exchange between end-to-end were performed. In consecutive session, the key is constantly being replaced, and the server does not know any user's key throughout the process cycle. It only will appear as a single message along with a key and the key is not repeated to prevent message interception. The encryption process cycle is explained as below:

Three sets of public and private key pairs generation:

- **Identity Key Pair**
- **Curve25519 Key Pair**

Signed Pre-Shared Key with a mid-term Curve25519 key pair, which were generated during installation time and signed by the identity key were periodically rotated.

One-Time Pre-Keys with a One-Time Curve25519 Key Pair sequence, which generated during the installation time and will be reinforced when there is insufficient.

The session key is designed as below:

- **Root Key,** 32 bytes are used to create a chain key
- **Curve25519 Key Pair,** 32 bytes are used to create a message key
- **Message Key,** 80 bytes are used to encrypted the message content consists of, 32 bytes (AES-256 key), 32 bytes (HMAC-SHA256 key), 16 bytes (IV)

The encryption algorithm used are briefly described as below:

What is RSA?

RSA (Rivest-Shamir-Adleman) is an algorithm for public-key cryptography invented by Ron Rivest, Adi Shamir and Leonard Adleman in 1977. It works on the basis of a public and private key. In RSA cryptography, both the public and private keys can encrypt a message. Example, User key A used to encrypt the message can be decrypted by using the same key. It provides an approach to ensure the confidentiality, integrity and authenticity of the data.

What is ECC?

ECC (Elliptic Curve Cryptography) is an alternative mechanism for implementing public-key cryptography invented by Victor Miller and Neil Koblitz in 1985. It promises stronger security, high performance yet shorter key lengths. ECC is a method to encrypt data so that only specific person can decrypt it. For example, to ensure only recipient can read the message when an email is sent.

What is SM2/SM3/SM4/SM9?

SM2 is a 4-part standard for public key algorithms based on elliptic curves specified by China. SM3, a hashing algorithm similar to SHA-256, and SM4, a block cipher algorithm for symmetric cryptography similar to AES-128. It is often used in commercial applications such as telecommunications and banking. SM9, an identify-based cryptographic algorithm with bilinear pairings These are commonly used for generate and verify digital signatures.

The overall mechanism flows are shown as below:

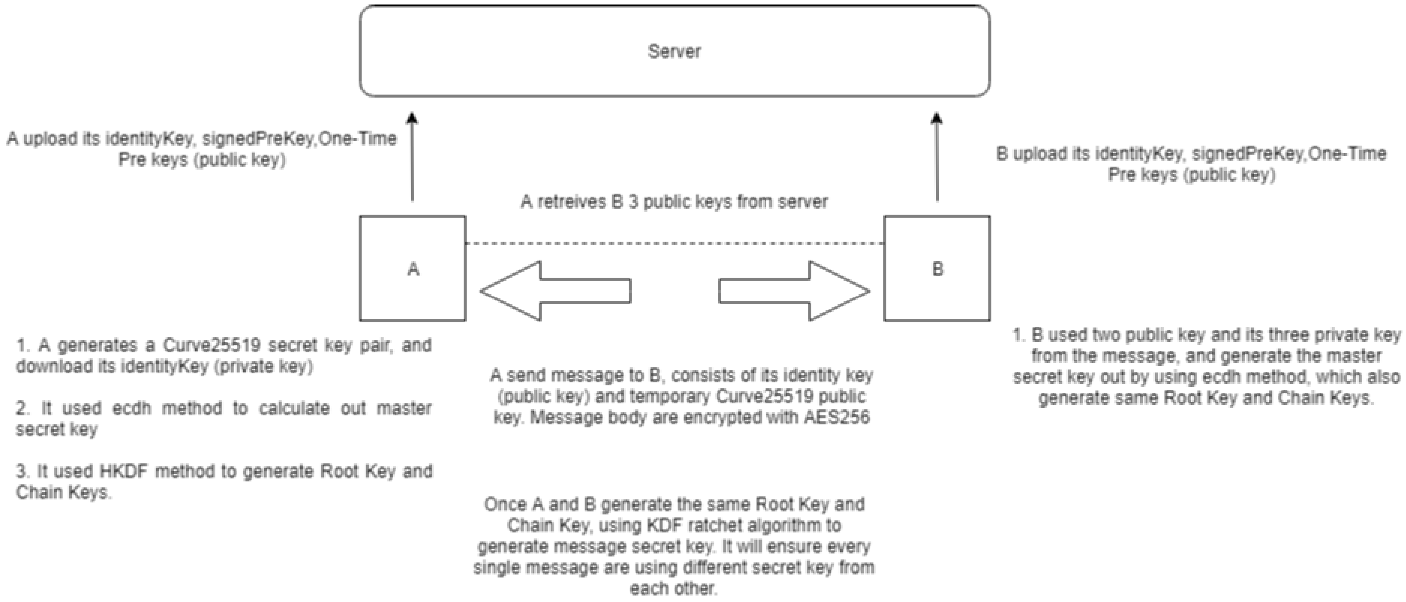

Server
A upload its identityKey, signedPreKey,One-Time Pre keys (public key)
B upload its identityKey, signedPreKey,One-Time Pre keys (public key)
A retreives B 3 public keys from server
A
B
1. A generates a Curve25519 secret key pair, and download its identityKey (private key)
2. It used ecdh method to calculate out master secret key
3. It used HKDF method to generate Root Key and Chain Keys.
A send message to B, consists of its identity key (public key) and temporary Curve25519 public key. Message body are encrypted with AES256
1. B used two public key and its three private key from the message, and generate the master secret key out by using ecdh method, which also generate same Root Key and Chain Keys.
Once A and B generate the same Root Key and Chain Key, using KDF ratchet algorithm to generate message secret key. It will ensure every single message are using different secret key from each other.

Figure 7

In the beginning, User A and User B upload their own three public keys to the server so that the other party can obtain them. A generates an elliptic curve algorithm Curve25519 key pair, and encrypt the private key with the identity key. From server database side, the secret keys are generated by using a random generator method such as hashing and Salt along with others parameter (timestamp, user info etc).

Next, A uses the ECDH key negotiation algorithm to generate the master key master_secret and then uses HKDF (Hash-key derivation function) algorithm to generate a root key and chain key. A sends a message to B, consists of its identity key (public key) and a temporary Curve25519 public key. The message body are encrypted with AES256. The transmission channel used https – TLS 1.2 along with RSA/ECC/SM2 encryption and the secret key are not kept in there since it is using HTTPS protocol.

B used two public key and its three private keys from the message, and generate the master secret key out by using ECDH method, which also generate same Root Key and Chain Keys. Once A and B generate the same Root Key and Chain Key, KDF ratchet algorithm will be used to generate message secret key. It will ensure every single message are using independent secret key from each other. Secret keys are send to recipient via message channel The generated Root Key and Chain Key only exist on both endpoints of A and B. It will not send and stored into the server or any other third party, ensuring that the key is not obtained by any third party, and thus achieved a secure end-to-end encryption.

Hardware-based encryption

LiNKDOOD also provides hardware-based encryption for TF (TransFlash) card on per request basis which offer encryption and decryption interface. Hardware-based encryption supports a strong encryption security with a minimal configuration requirement and platform interoperability. It separates the authentication and encryption task individually between hardware and software in result of accelerated algorithm processing, tamper-proof/resistance key storage and act as a shield to protect against unauthorized code which could potentially exploit the software security algorithm. TF card store encryption key in the chipset and act as an interface to perform encryption with SM9 identify based encryption.

How does this approach changes the existing enterprise traditional system

With the newly-defined IM-DNS routers, LiNKDOOD can communicate with different IM applications through an IMTP protocol. Hence, in the same spirits as an email system which allows users to literally break communication barriers between IM system. With technologies such as data encryption, communication security and cross-regional communication, LiNKDOOD ensures a secured and instant communication between users across different platforms, regions and organizations, thus enhancing the safe and rapid upload/delivery of data. Nevertheless, LiNKDOOD possess an array of opened APIs which allow for the secured integration of industry-focused applications.

Conclusion

This new approach offers a better secured communication for enterprise with reduced risk of data compromised and greater efficiency compared with today's enterprise information security. With the consecutive development of internet technology along with its security scale, security requirement gradually become progressively prominent especially in enterprise financial, e-commerce, daily conversation and storage/database etc. With the traditional method to solve the security issues, the drawback is great. Many enterprises should be aware of the importance of data confidentiality, privacy and sensitivity. Therefore, data encryption and communication architecture is very important as it could greatly maximize enterprise data security.