International Journal of Research in Engineering and Innovation (IJREI)
journal home page: http://www.ijrei.com
ISSN (Online): 2456-6934

ORIGINAL ARTICLE

Security analysis of swift financial software

Neetu Rani Sharma[1*], Harshita Kamboj[1], S.K. Gupta[2]

Department of Computer science and engineering, Neelkanth Institute of Technology, Meerut, India.
Department of Computer science and engineering, Bhagwati Institute of Management & Technology, Meerut, India

Article Information

Received: 07 June 2022
Revised: 21 Aug 2022
Accepted: 29 Aug 2022
Available online: 04 Sep 2022

Keywords:

Security analysis
Swift communications
Swift software business
Flow data

Abstract

Our lives depend heavily on banking, and the modern financial systems are the foundation of any nation's development. Government laws need quick and secure financial transaction solutions for all company types. Every bank has a robust security system as part of its software or operating system. Still, we cannot alter other banks' systems and are unaware of their security protocols. In such circumstances, we want a reliable mechanism for conducting payment transactions with overseas banks. Swift is an intrabanking transaction system application. But each method has specific benefits and drawbacks. We will examine the Swift Software System's operation in this study and make some modifications to increase financial transactions' safety and security, utilising more sophisticated token-based authentication systems and encryption techniques.

1. Introduction

Swift stands for (the Society for Worldwide Interbank Financial Telecommunication). Swift is an international money transaction system to send money to other country. This software is the best path for online money transaction to other bank. Swift is a very helpful software for solving the problem of an ordinary layman [1-5]. Central bank and other commercial bank use it. Swift provides best services to our society, by providing financial services such as rapid financial transaction and payments. This service is very fast and reliable, secure and helpful that saves time and people utilize their saved time in other developmental activities, that leads to economic Growth. The SWIFT financial system was established on May 3, 1973, in Brussels, under the supervision of its first CEO, Carl Reuters Ki old. The system is backed by 239 banks in 15 countries across the world. Prior to it, international financial transactions were transmitted using Telex, a public system that included manual drafting and reading of messages, which increased the cost of both time and money [6-9]. SWIFT is governed by the G-10 Central Banks, which include the United States, United Kingdom, Canada, Belgium, France, Germany, Italy, Japan, the Netherlands, Switzerland, and Sweden, as well as the European Central Bank. Swift's headquarters are in La Hulpe, the Belgian National Bank. The SWIFT framework was revised in 2012, and central banks from additional large economies joined the G-10 [10, 11]. Banks from other major economies include the Reserve Bank of India, the Reserve Bank of Australia, the Bank of Russia, the People's Bank of China, the Hong Kong Monetary Authority, the Saudi Arabian Monetary Agency, the Bank of Korea, the Singapore Monetary Authority, the Central Bank of Turkey, and the South African Reserve Bank [12-18].

1.1 Transaction Life Cycle of a Documentary Credit

A Documentary credit transaction will originate with the issue of a (LC) through MT 700. Let’s start with this. In MT 700 the

**Corresponding author: Neetu Rani Sharma*
Email Address: sharma.anamika2010@gmail.com
https://doi.org/10.36037/IJREI.2022.6505

field length is pre-defined and standard. The users may face the field length limitations in respect to filed No. 45A – Description of goods, Field No. 46A – Documents Required and Field No. 47A – Additional Conditions. Few Banks use free format messages (to provide full details of fields 45A, 46A and 47A which is not correct. When the field length is exceeded, the users must use MT701 as a continuation of these three fields. Modification of Credit letters are very familiar. These are addressed under Article 10 of UCP and transmitted through MT707 – if, stated in the original Letter of Credit, reimbursement is provided through MT740 and if the amendment affects the contents of MT740, an MT747 must be sent to the reimbursing bank [19-22]. The MT700 receiving bank (advising bank) is expected to acknowledge the receipt / advise of LC and such acknowledgement is transmitted through MT730 wherein they incorporate their reference number in Field No.20 with the corresponding issuing bank reference number in Field No. 21 [23]. An internal policies and trade practices, completely depends on their emerging banks. Incorporate reimbursement instructions on how they will reimburse the negotiating bank. In non-confirmed LCs, banks will often offer to remit the proceeds under LC complying presentation as per the instructions of the negotiating bank. In confirmed LCs, though, the confirming bank will seek a reimbursement claim. In such cases, the issuing bank will incorporate and authorize the negotiating bank to claim from the reimbursing bank. In such instances, the issuing bank must send the Reimbursement Authorization to the reimbursing bank [24, 25].

Figure 1: Image of SWIFT

1.3 Literature review

Rahul & Abhineet Anand, since the late 1990s, internet banking systems have caught the attention of banks, securities, and insurance companies in developing countries. Given the significant and quick expansion of the electronic sector and of commerce, it is obvious that electronic (online) banking and payments are likely to advance or increase quickly. You can handle your finances whenever you want, around-the-clock, 365 days a year, thanks to Internet banking. Safe and secure: We take client security extremely seriously and take all reasonable precautions to ensure it. Improve the speed of your applications: -Using the Internet Bank to apply for goods is quicker because we already know you. At any time, you can access your balance, available balance, and statement history. Use your credit card wisely. View direct debits and set up recurring payments. Requests for overdrafts will be answered right away (subject to approval). Keep an eye on your mortgage or loan account.

To lessen the possibility of stealing a client's money, two key security layers are added: transaction authorization and client authentication. Once the attacker has the client's login information, he will also need the authorization password in order to steal the client's money. Passwords for authorization should be linked to transaction information. When this is the case, even if the attacker obtains the authorization password, he cannot execute any arbitrary transaction. The attacker is then rendered worthless by phishing. When the client's system utilized for transaction verification is still infected, the issue is malware. Modern cellphones first appear to be a viable option for transaction verification because they are widely used and no additional device is required. However, they are multipurpose gadgets with the same security issues [26]. Mohd hamid and M. Kabir Hassan, private computers. Therefore, it is suggested to employ a This study provides a thorough analysis of the expanding body of research examining the problems associated to the financial system's exposure to cybersecurity risk. As a result of the cyber security risk becoming a serious concern to the financial industry, researchers and analysts are attempting to approach the issue from several angles. There is a tone of materials available that include conceptual ideas, technical analyses, and survey results, but there aren't many real studies using real data just yet. Additionally, the global and national. Regulating agencies create guidelines to assist banks and financial institutions in reducing their exposure to cyber risk. In this essay, we summaries pertinent publications and policy documents on cybersecurity risk, focusing on aspects that increase the vulnerability of the financial sector. [27]. Petrit Hasanaj1 & Beke Kuqi2 -The major goal of this study is to ascertain, anticipate, and evaluate the greatest possible economic circumstances and business performance in the future. The financial statement will be analyzed as part of this study's secondary goal, which is to provide financial managers with accurate information they can use to make decisions regarding their companies. The financial information uses instruments, analytical methodologies, and necessary business practices. It serves as a clinical tool for assessment. Decision-making, financial analysis, financial reports, profitability, and liquidity. [28]. Ashwini Sheth and Farish Kurupkar, It is essential to understand cyber security and be able to apply it successfully in the modern world, which is run by technology and network connections. If there is no security to secure it, systems, vital files, data, and other important virtual items are at risk. Every

business, whether an IT firm or not, needs to be protected equally. The attackers do not fall behind as a result of the advancement of new cyber security systems. They use improved hacking methods and target the weaknesses of numerous companies worldwide. Military, governmental, financial, medical, and corporate institutions collect, use, and store huge volumes of data on PCs and other devices, making cyber security crucial. Sensitive information, including financial data, intellectual property, personal information, and other types of data for which unauthorized access or acquaintance could have unfavorable effects, can make up a sizeable portion of such data. There are three main goals. 1. Protecting information privacy 2. Preserving the Information's Integrity 3. Limiting Access to Information to Approved Users [29]. Muhamad Baqir, this essay examines the origins of all of these changes and how SWIFT has enhanced its procedures. What further suggestions may be made to improve the security of this network going forward? SWIFT, digitization, international settlement, and cybersecurity The term "digitalization" refers to the process of upgrading or converting financial data into a digital format and making it accessible online, more specifically, making the information and data available online. In the beginning, this was mainly accomplished through the use of digital accounts, ATMs, electronic trade, worldwide payment networks, online banking, and, most recently, mobile payments. This essay covered the SWIFT network's use of cyberattacks as a message-instruction mechanism for financial systems. This research also looked at what may have been done to strengthen this network's cybersecurity. After all, in order to combat SWIFT itself has also proposed the creation of a SWIFT-managed VPN infrastructure.

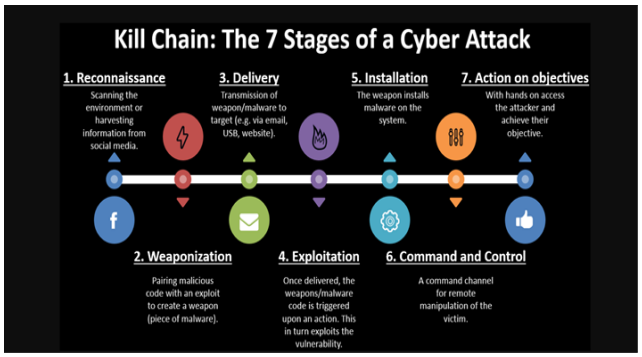

Figure 2 cyber kill chain

S. M. Ikhtiar Alam, Ph.D. The information in this handout demonstrates how SWIFT operates in practical circumstances. Need to send money abroad? Today, walking into a bank and sending money anywhere in the world is simple, but how does that work? The SWIFT system is responsible for the majority of global financial and security transfers. Banks and other financial organizations utilize the extensive messaging network SWIFT to send and receive information securely, promptly, and for money transfer orders [30, 31]. Susan Scott and Markos Zacharias's How does a significant financial network innovation affect the performance of a company? Although there has been much speculation, there is little solid quantitative data regarding how technology dispersion has affected the financial services industry. In this study, we use bank-level panel data for the US, Canada, and 27 European nations along with the complete adoption history of SWIFT (the Society for Worldwide Interbank Financial Telecommunication, a standards provider and messaging carrier). Between 1998 and 2005, our dataset includes over 7,000 banks, including 1,689 SWIFT adopters. Our findings support the notion that there are considerable synergies between new technologies and company structure because adoption seems to have a big impact on profitability, but it takes time before any good return is apparent. The profitability effect is stronger for smaller businesses than for larger businesses and works by increasing revenues while lowering operational costs. The US and UK banks seem to benefit from adoption more swiftly than their Continental European rivals, despite the fact that the long-term consequences are similar. This supports the notion that because transition costs are lower in the US than in Europe, the impact of information and communication technologies is greater there. [32]

2 Methodology

In order to enhance international financial transactions, researchers have utilised far more sophisticated technologies, such as hacking, malware, social engineering, integrated cybercrime, SWIFT, digitalization, bank operating risk, IT expenses, banking sustainability, cyber risk, and global data security. Encryption of data. The researchers' technique includes biometric verification and multivariate regression verification.

2.3 Outcomes

Suppose you work for a financial company, bank, or technology company. In that case, we hope our concise evaluation will assist you in identifying the best option for your SWIFT library requirements. Payment components, of course, would be happy to answer any more questions you may have about Swift financial massaging and provide you with a precise price quote customised to your specific needs.

3 Swift structure and message

Three headers, the message content, and a trailer are the five components that make up a SWIFT message. They are distinguished by complementing descriptions. A three-digit number designating the message categories, group, and type is always followed by the letter MT, which stands for Message type, in all SWIFT exchanges. For each communication type, SWIFT offers predefined formats throughout the transaction lifecycle [8]. Messages that fall under every one of the criteria mentioned above are in the category. Payments, interest, as

well as other modifications guidance, are found in MTn90.
MTn99: Bank frequently utilize
MTn98: Proprietary message
MTn96: Response
MTn95: Inquiries
MTn92: Request for cancellation
MTn91: Interest, charges and other expenses

SWIFT users are encouraged to employ structured messages throughout the transaction life cycle since they can be advantageous to them.

MT9nn	Customers status and cash Management
MT8nn	Travelers Cheques
MT7nn	Documentary guarantees and credits
MT6nn	Syndications, and Precious metals
MT5nn	Securities markets
MT4nn	Collection and Cash Letters
MT3nn	FX, Money Market and Derivatives
MT2nn	Financial Institutions Transfers
MT1nn	Customer Payment
MT0nn	System Messages

The first digit represents the category. A category denotes a group of messages concerning the same product or service. The whole list is seen below. Swift communications are recognised using standardised techniques. Each one starts with the message's abbreviation, "'MT."

Table 1: Message type format

MTn99	Free format
MTn98	Proprietary message envelop.
MTn96	Answer
MTn95	Query
MTn93	Directory services
MTn92	Request for cancellation
MTn91	Request for payment of charges, etc.
MTn90	Advice of charges, interest etc.
MT999	General free format
MT599	Free format relating to transfers
MT299	Free format relating to transfers

4 Swift's business and importance

4.3 Swift software business consultancy services

It has a broad range. It makes it easier to integrate international financial transactions securely. We pioneered the practice of organising an IT consulting organisation around vertical companies. Over the years, we've gained broad and in-depth experience in almost every primary industry, which enables us to foresee consumer demands and satisfy them whenever they materialise. In order to provide services from the front office to the back office and throughout the technological stack, we use the most modern tools and processes. We are dedicated to staying on the cutting edge of commercial and technical advancements in order to offer our clients the most outstanding results. With senior staff who have, on average, more than 15 years of experience in their respective industries and leading businesses, we provide high-level, experienced advice to stay in today's competitive climate.

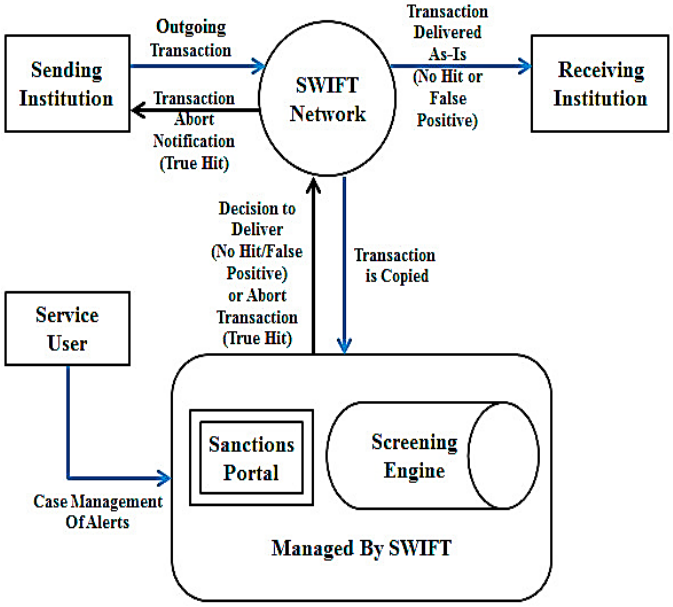

Figure 3: SWIFT messaging work flow

4.4 Swift's importance

To have access to the cost advantages of a best-in-class technology company and the deep strategic capabilities of a top global consultancy. Our business and technology-trained consultants collaborate closely with delivery teams to bridge the IT-business gap, and our consulting practice is well established in our sector. As a result, original, imaginative, and valuable ideas are created to maintain global competitiveness. In addition, the factors listed below highlight SWIFT's significance on a worldwide scale. Swift 2.0 is required for globalisation. We can effectively and efficiently meet your most important requirements by utilising the best and brightest ideas and resources available. The location's exactness becomes crucial in Swift 2.0. Resources can be accessed locally, nearby, or at our worldwide distribution centres. Everywhere in the globe, there are places for us. In today's modern economy, cost savings are necessary to foster corporate development and innovation. IT and business strategy are essential success elements for business value and technology.

4.5 Strategic Services

With the help of knowledgeable business professionals, create and direct your future business and IT goals and agendas across several sectors.

4.6 Business / it strategy

Please find out how changing your company processes with IT may give you a competitive advantage.

4.7 Application portfolio

Regarding restricting data mining, achieving maximum efficiency, and more for your IT applications and assets, as well as application pass-out retention, cost-effective efficiency, and more.

4.8 Transformation of global sourcing

Learn how to save expenses, enhance the effectiveness of IT processes, centralise operations, and consolidate vendors by utilising global and multi-sourcing approaches.

4.9 Process transformation and busniness operations

We help you with process analysis, redesign, and outsourcing for strategic objectives, including time to market, right-sourcing, and strategic throughput.

4.10Operating model and it organization

Establish operational models and an IT structure that aligns with corporate objectives.

4.11Organization change management

The change management process's transitional, communications, organisational, governance, and behavioural components must all be addressed. Integration Following a Merger Through careful communication planning, goal state definition, implementation planning, and transformation management, ensure your company is integrated.

5 Implementation of security of swift

Society for Worldwide Interbank Financial Telecommunications proves its importance in last several years. But we can't have forgot the following attacks in SWIFT:

- In 2013 Sonali Bank Bangladesh ($250,000)
- In Jan 2015 Banco del Austroz, Ecuador (12 Million Dollar)
- In Oct 2015 Philippines
- In Dec 2015 Tien Phong Bank, Vietnam (1.13 Million Dollar)
- In Feb 2015 Bank of Bangladesh (81 Million Dollar)
- In 2015 Again Ukranian Bank Ukrain (10 Million Dollar)
- In October 2017 Taiwan (60 Million Dollar)
- In October 2017 Asia Bank, Nepal (4.4 Million Dollar)

There are some security breaches in the working of SWIFT. After studying and researching all these attacks in details we found following factors are responsible for the attacks:

- Malware Deployment
- Possible Insider Threat
- Employee Email Access
- Unknown Attack Vector
- Lateral Movement
- Credential Compromise

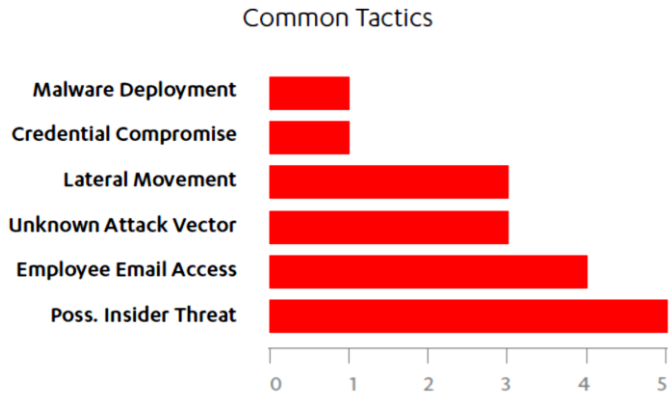

Figure 4: Factors Responsible on Scale of 5

It shows that none of the attacks directly compromise the SWIFT Network itself; 95% of Errors are due to humans. But we can't ignore the 5% part of the SWIFT Security system itself.

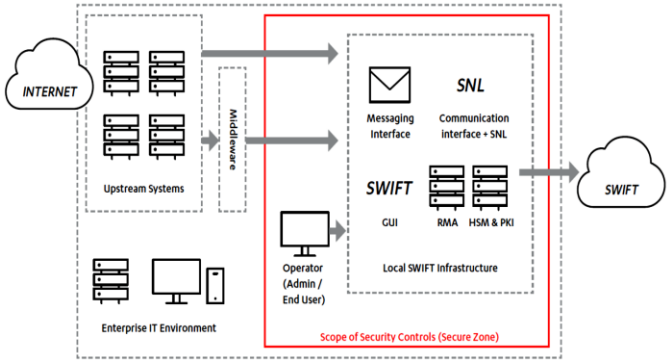

Figure 5: Full Stack Swift Infrastructure

- Data exchange layer: This layer handles data interchange between local swift infrastructure and upstream systems or middleware.
- Secure zone: This network segment isolates quick systems from the rest of the business environment.
- Messaging interface: This is software that supports using the messaging service provided by Swift. Normally, this is immediately connected to the communication interface.

- Communication Interface: This is a software product (such as Alliance Access) gateway that establishes a connection between the messaging interface software and the Swift Network (Swift Net).
- Swift Net Link (SNL) is a 5. - This programme must be used in order to use messaging services via a secure IP network (With in the above diagram the SNL is part of communication interface).
- Connector: A local software product, such as the alliance lite two auto client, that enables connectivity with a message and communication interface is known as a connector.
- HSM& PKI: This is the critical public infrastructure and quick hardware security mechanism.

Following are the possible key points of attacks: Implementing more security and using Strict suggestions of Complex Password and avoiding Malwares can improve the security by 95%. But we can't say that this is sufficient. Following is the General Attacking Methodology

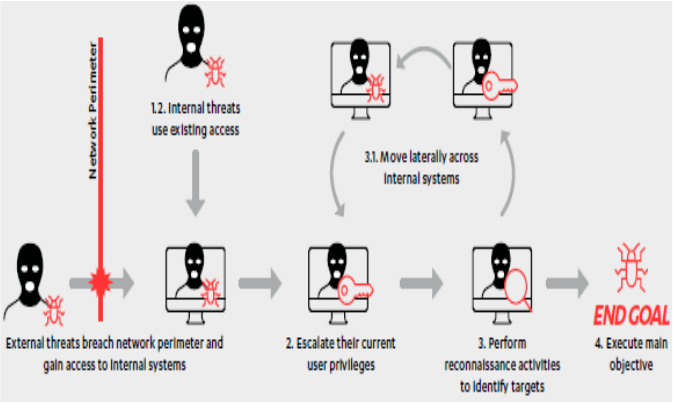

Figure 6: General Attacking Methodology

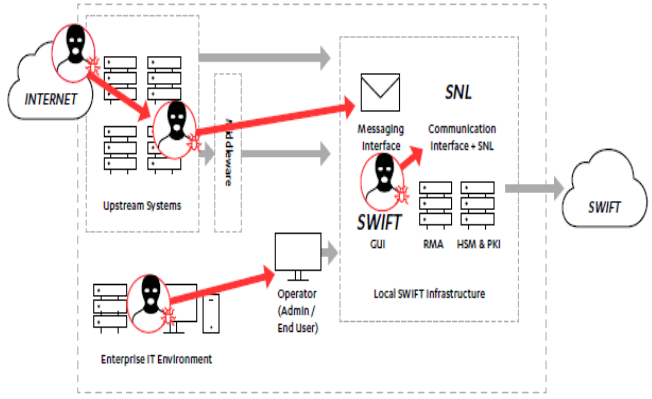

Figure 7: Attack Vectors Weak Security

After Researching each factors and point of security attacks we suggest following Steps:

1. Prevent
2. Detect
3. Respond
4. Predict

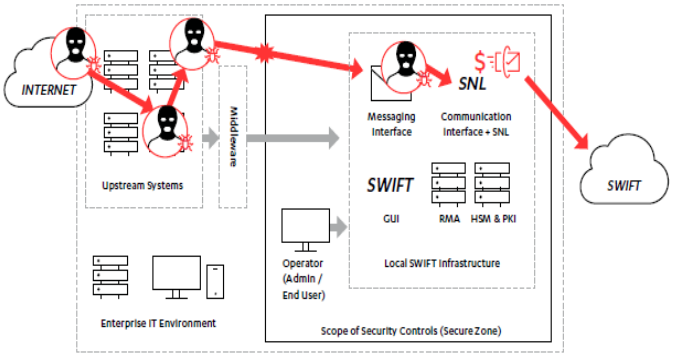

Figure 8: Attack Vector (After Security)

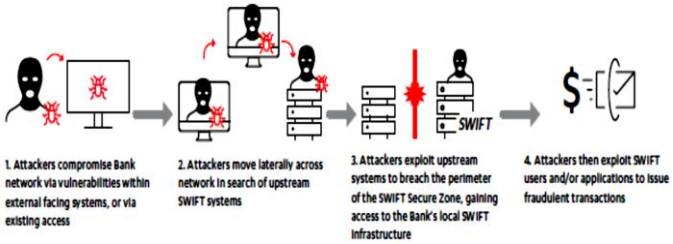

Figure 9: Hypothetical Attack Scenario

5.3 Predict

Prediction is the most important point to map the possible attacks within the Financial Institutions. An attacker always compromises the network of the Institution or Swift Security System. We suggest that we perform reverse process to predict the problem or attack scenario. Starts from the SWIFT structure with implemented security system and after that infrastructure of Financial Institution. Study all points of communication and connections. Also include the working model of the Institutions with Management Work Culture. Internal Software must be test for any penetration and this task should be monthly or quarterly. Any penetration attack should not be available to public but it should be kept secret and make sure to solve that problem.

5.4 Prevent

Once we found each and every points of attacks, next step to prevent these attacks by providing proper security and by changing the work culture of the Financial Institution.
Setting up measures to stop malware execution should also receive much attention. These controls should also be backups in case one fails or is disregarded. e.g.:

- Mail Gateway
- Endpoint Devices
- Account Control

Mail Gateway- Very High restricted control. Each and Every Incoming and Outgoing email should be check for attachment and the contents of attachment. Only some type of files

allowed for out. Endpoint Devices - Execution of Macro, Scripts and binary files should be in control of the Administrator. Account Control Removal of unused accounts, removal of extra privileges and implementation of Multi-factor authentication.

5.5 Detect

The ability to recover from these cyberattacks depends heavily on prompt action, made possible by an effective attack detection technique. It is no use to learn that a compromise has occurred after reading a day's end report. Financial institutions must establish comprehensive logging for all virtual servers in the environment and use endpoint detection and response (EDR) technology to keep track of servers and endpoint devices. Additionally, MWR advises that organizations use a threat hunting strategy to detect and ensure that threat hunters know about payment systems and all known attacks against SWIFT networks. Endpoints utilized by privileged users should be prioritized, as they are the endpoints most likely to be attacked by sophisticated threat actors.

5.6 Respond

These detection and reaction skills will ultimately decide the total financial effect of a hacked institution's local SWIFT infrastructure if preventative efforts fail. Investing resources in developing a mature detection and response plan around your SWIFT implementation and its upstream systems is crucial. The primary objective is to stop an attack and recover from it effectively. Financial institutions should regularly perform incident response drills to ensure that the policies and processes enable quick reactions to an issue. This should involve comprehensive incident response run-throughs based on SWIFT systems and tabletop exercises to test these processes. Case studies are crucial; to stop future attacks, we must look at previous assaults and their reports.

6 The working of the protocol is as follows

- If S and R desire to communicate, S sends a message to R that contains both their identification numbers, IDS and IDR, and a message that has been encrypted with MS's public key, KUMS. An IDS, IDR, and nonce NS created by S for this communication session are all present in the encrypted message.
- R produces a nonce NR for this communication session after receiving this message, concatenates it with IDS and IDR, and encrypts it using KUMS, the public key of MS. R transmits this encrypted message to MS after concatenating it with the message it originally got from R.
- Using its private key KRMS, MS decrypts these two encrypted portions of the message and compares the results with IDS and IDR. After verification, it creates two messages, one for S and one for R, for each conversing party. The message for S contains S's nonce (NS) and S's public key (KUS) and nonces are obtained by decrypting a portion of the message using KUMS. To ensure that the public key is for the appropriate communication session, it verifies NR. It then uses its private key to encrypt the NS that was previously obtained (KRR). It then joins the KRMS-encrypted portion of the message received from MS with the encrypted NS before sending it to S.
- After receiving the message, S uses KUMS to decode the relevant portion of the message to obtain both the nonce and R's public key (KUR). The other piece is subsequently decrypted using its private key so that NS may be retrieved. S is therefore reassured that R transmitted the message and that the public key is valid for the intended communication session. It then encrypts NR with R's public key (KUR), sending it back to R to prove its identity.
- R receives this message, decrypts it with KRR, and is thus satisfied that S has successfully received its public key.
- Using their private-public key pairs, A and B may now interact with each other on the unsecured network in a legitimate manner.

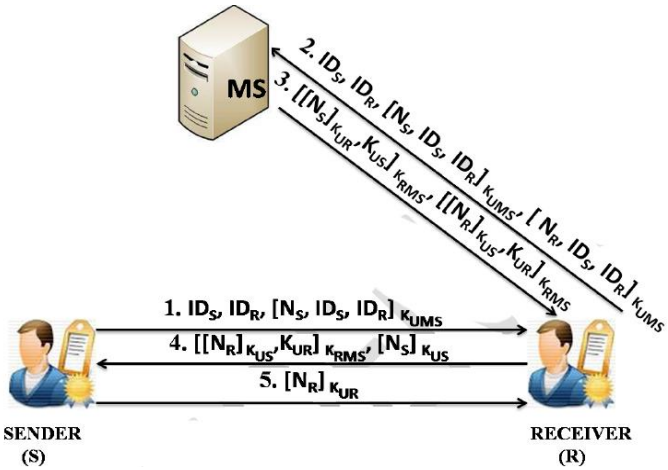

Figure 10: Proposed protocol overcomes the cloud security problems

6.1 Public Key Distribution

In the proposed protocol MNSOR the secure public key distribution is completed with the help of mutually trusted third-party MS.

6.2 Authentication

The authentication is covered in steps 4-5 of the MNSOR protocol for the communicating parties. Receiver R encrypts the nonce of Sender S (NS), generated by using the sender's public key. After that, the sender encrypts the nonce of the receiver (NR) by using the public key of receiver R and sends it back to R to complete the authentication process.

6.3 Clock synchronization

In a cloud-distributed environment, many networking devices are performing their role to complete communication, which is why it isn't easy to synchronize their local clocks in the entire network. MNSOR protocol removed the dependency on timestamps for preventing replay attacks, so there is no requirement for clock synchronization.

6.4 Utilization of Server Time

In the proposed protocol, both the communicating parties are ready before verifying the identities of sender S and Receiver R by the trusted third-party server MS. After this, the MS distributes the public keys.

7 Future Scope

7.1 Business intelligence smart to your needs

SWIFT scope uses data a collected from SWIFT communications and other relevant sources to give business intelligence solutions suited to your needs, utilizing up-to-date technology and experienced business understanding. SWIFT scope is straightforward to adopt and has a small footprint. It's deployed on your premises so you're always in control. It can handle all aspects of data collection, transformation, storage, and display, depending on your requirements. To add value to your study, you may integrate SWIFT message data with additional reference data, such as bank and legal entity identification and exchange rates/pricing data, using SWIFT Scope.

7.2 Cross-Border flow data and analysis to support central banks

Central banks keep an eye on markets and transaction flows to understand the effects of monetary policies, achieve prudential and regulatory goals, and advance their respective national economies. To obtain the data they need, central banks anticipate that commercial banks will report payment movements more often and in detail. Both central banks, which must collect and analyze data, and registering banks, which must acquire, process, and report large amounts of data, are subject to financial and resource restrictions.
A business intelligence platform called SWIFT Scope for Central Banks was created expressly to meet central banks' data collection and analysis requirements. The system automates the gathering and analysis of cross-border transaction flow using SWIFT message data. It can also collect and integrate data from other information sources to provide complete and thorough coverage of cross-border activities. The information is gathered and kept in a data warehouse on the premises of the central bank, where it may be examined as required. SWIFT Scope for Central Banks allows central banks to gather and analyze payment data more rapidly and effectively. The overhead of manual data processing associated with routine central bank reporting of participating commercial banks' transaction flows is also reduced.

7.3 Investigational Options

With the help of SWIFT Scope's flexible analytical and data visualization capabilities, users can create information dashboards that are simple to grasp and offer significant insights.

- Review payment trends,
- Dynamic transaction monitoring in real-time
- Monitor the status of your financial flow.
- Identify unanticipated monetary inflows and outflows.
- Investigate anomalies right down to the transaction level.

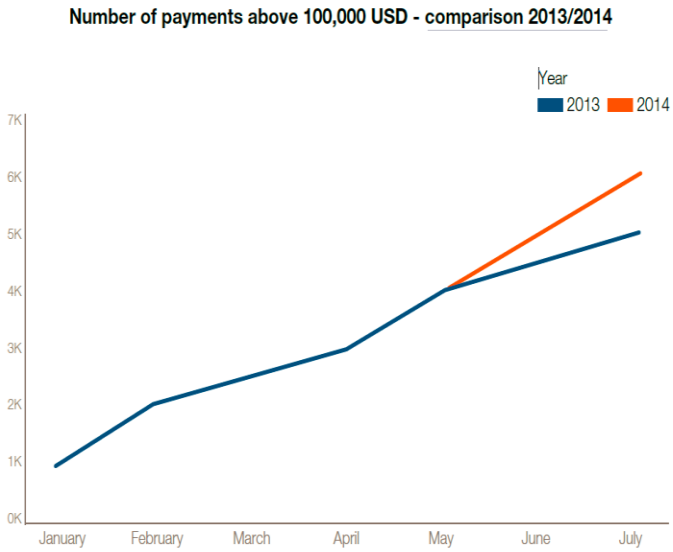

Figure 11: payment growth

8. A Flexible, End-to-End Encryption

8.1 Central Banks' SWIFT Scope

It's a versatile on-premises solution that gives you total data control. It's simple to set up and includes project management from start to finish, software installation and configuration, end-user training, support, and maintenance. A complete architectural evaluation and integration service may be performed based on the customer's needs.
Why not contact us if you're a central bank searching for a business intelligence solution? We'd be delighted to discuss how SWIFT Scope for Central Banks may help you.

9. Swift scope technical factsheet

9.1 Business intelligence solution

Business intelligence fact sheet swift scope is a lightweight and simple-to-implement end-to-end business intelligence solution implemented on your premises. SWIFT Scope encompasses all aspects of data collection, transformation, storage, and display. Because of the solution's versatility, you may choose the combination of services that best meets your needs, whether it's historical data analysis or dynamic transaction monitoring. For participating commercial banks, the burden of manual data processing connected with regular central bank reporting of their transaction flows is also minimized. SWIFT scope project includes end-to-end project management, guided software installation, and end-user training to guarantee a cost-effective implementation tailored to your individual needs. technical requirements SWIFT Scope is a SWIFT-based business intelligence tool that may incorporate reference data from a variety of sources.

SWIFT Scope pulls data from your SWIFT interface, such as payments, trades, and securities communications. By using an automated copy, the system may also aggregate communications delivered via the SWIFT network from other participating institutions (e.g. automatically copy branch activities to group headquarters). The analysis can include any SWIFT message (FIN/InterAct/FileActSWIFT) Scope then processes and normalizes all of the data, resulting in a business intelligence-ready data format. Data processing is completely automated, and data from many sources may be added (bank reference data, exchange rates, etc.). A variety of data visualization options might assist you in gaining important insights into your company's operations. Outliers, trends, and danger may all be easily identified using customized information dashboards. This data, presented in a simple, graphical fashion, offers decisive assistance for better business decisions.

- End-to-end solution
- Automated, customizable, and safe
- Visualization and analysis
- Data transmission in real time
- Information from a variety of sources

Without the specific authorization of both the sender and receiver of the SWIFT message, no data is copied. Sending a Bank SWIFT Message to a Customer Automated copy of a SWIFT message.

9.2 SWIFT Today

SWIFT was founded in 1973 by 239 banks from 15 different countries and began by offering messaging services in 1977. Banks can exchange information on financial transactions using the SWIFT net messaging system. Financial institutions communicate information, including payment instructions, using SWIFT in a secure manner [33]. Over the years, SWIFT has grown to provide various services outside the internet messaging system. These include market infrastructure, compliance, and cloud-based connection [9]. Economic sanctions can no longer utilise SWIFT's services because of their integration with global cash movements. Due to economic sanctions placed on Iran by the European Union because of its nuclear weapons development, SWIFT cut off access for Iranian institutions in 2012. In 2016 [10], it reopened access to Iranian banks that other sanctions had not hit. In retaliation for Russia's invasion of Ukraine in 2022, SWIFT banned several Russian banks. The member-owned cooperative SWIFT offers secure messaging for international money transfers (Society for Worldwide Interbank Financial Telecommunications). Over the years, SWIFT has grown to support more than 11,000 institutions working in more than 200 nations [1]. SWIFT handled 42 million messages daily in 2021, an increase of 11.4% from 2020.

10. Technical Specifications

Quick scope is a swift message-based business intelligence tool. Swift scope source data such as payment, trade, or securities messages from your swift interface may be included. Using automatic copy, the system may also condense messages delivered over the fast network from other participating banks. The study has taken into account any urgent messages. Swift scope processes and normalizes Ll data. Creating data for the purpose of business intelligence. The data processing is totally automated, and it includes information from a variety of sources. A range of data visualization techniques can help you get important insight into your business operations. Outliers may be easily identified with customized information dashboards.

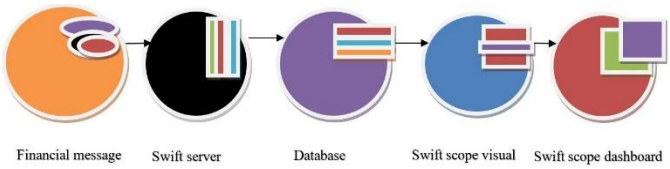

Figure 12: Outliers

10.1Financial Messaging

All quick messages are automatically and transparently strengthened and included in your analysis. Group headquarters copies all incoming and outgoing branch communications. Notification of debit and credit transactions to banks for liquidity monitoring.

10.2Swift Interface

SWIFT connect networks are used to manage the sending and receiving of quick messages. It is feasible to install current junction access and lite parts.

10.3Swift Integration Factors

It converts quick data into a format suitable for optimum analysis.

10.4Database Server

It stores all fast business intelligence data, as well as reference data and non-swift data sources.

10.5Swift Scope Dash Board

All dashboard and report control data, access and permission support are generated by the visualization server. For user authentication and group membership definition, Microsoft Active Directory SAML 2.0 has a built-in user system.
All dash boards are intended for business users and are accessible via a web browser.

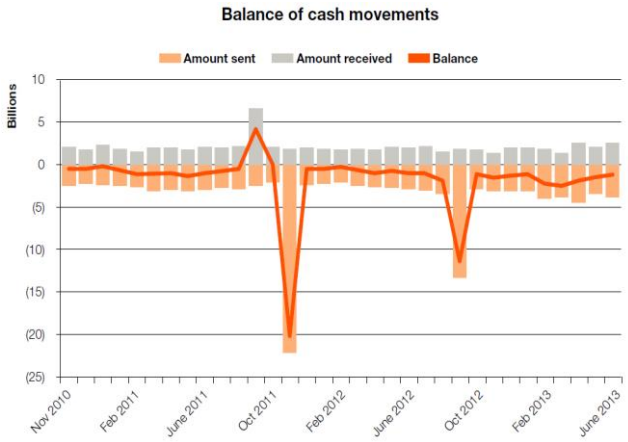

Figure 13: Graphically representation of cash balance

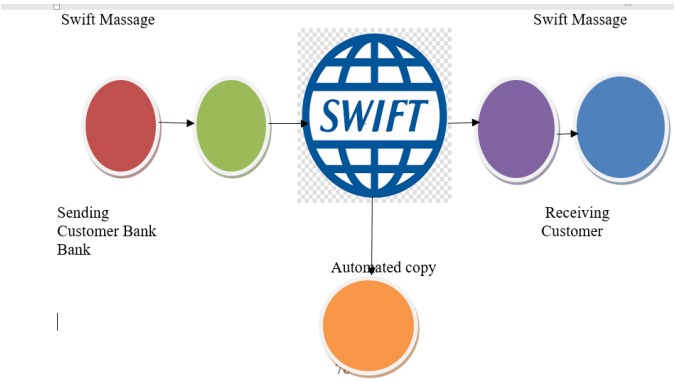

Figure 14: Data copied

11. Swift Payment System

- Financial transactions between institutions worldwide are facilitated and carried out by the Belgian cooperation SWIFT. International Money Transfer is another name for Swift Transfer. Instead of aiding with financial transactions, the SWIFT payment system communicates payment instructions that must be completed through correspondent accounts that institutions have with one another.
- As with Gmail, banks and other financial organisations utilise SWIFT, an international system, to send text messages, such as orders and confirmations for payments, transactions, and currency swaps.
- A few governmental financial institutions that regulate it are the US Federal Reserve System, the European Central Bank, and the National Bank of Belgium. The company's main office is in La Hulpe, France. Belgi, a city around Brussels
- SWIFT makes sure that financial communications are sent securely. It doesn't carry out clearing or settlement or keep accounts for its members.
- The SWIFT bank system also offers software and services to financial institutions, especially for use with its own "SWIFT Net" network and ISO 9362 Business Identifier Codes (BICs), also referred to as "SWIFT codes."

12. Conclusions

In today's digital environment we need safe and reliable Transaction System between Banks and Financial Institutions of all over the world, using that system they should perform financial transactions in easy and secure way. SWIFT is such software which proves its importance in some last couple of decades, but no one can be perfect and each system requires maintenance and security checks to prevent attacks. Attackers are evolving significantly in terms of sophistication, tenacity, and resourcefulness due to the enormous amounts of money available. Threat actors have regularly employed custom malware and cutting-edge techniques in some of the most high-profile assaults to carry out fraudulent financial transactions. Our two step approach can prevent the such types of attacks and help to improve the security system.

References

[1] S. Kamel. The Use of Information Technology to Transform the Banking Sector in Developing Nations. Information Technology for Development vol. 11 (4) pp. 305–312, 2015.
[2] M. Loonam, & D. O'Loughlin, D.An observation analysis of e-service quality in online banking. Journal of Financial Services Marketing, 13(2), pp. 164-178, 2008.
[3] L.F. Amboko, & J. Wagoki, Determinants of Adoption and Usage of Banking Innovations by Consumers for Competitive Advantage: A Case of Banks in Nakuru County. International Journal of Science and Research (IJSR) 3(10) pp. 1597-1601, 2012.
[4] R.N. Acharya, & A. Kagan, Commercial B2B Web Site Attributes within the Perishable Sector. Journal of Internet Commerce, 3(4) pp. 79-91, 2004.
[5] J. Okoth. "Fraudsters take home billion s from banks" .Nairobi: East Africa Standard 17th November 2019.
[6] K. Okiro, & J. Ndungu. The Impact of Mobile and Internet Banking on Performance of Financial Institutions in Kenya. Journal of Business and Management 16(9) pp. 146-1612013.
[7] C. Ngalyuka, The Relationship between ICT Utilization and Fraud Losses in Commercial Banks in Kenya. Nairobi: University Of Nairobi 2013.

[8] M. Vatis. (2009).Trends in Cyber Vulnerabilities, Threats, and Countermeasures, Sci Report, 25, 2009.
[9] N.O. Leder. Proactive Botnet Countermeasures An Offensive Approach. Bonn: Institute of Computer Science IV, University of Bonn, Germany, 2009.
[10] S.W. Njiru. A Framework to Guide Information Security Initiatives for Banking Information Systems, Kenyan Banking Sector Case Study.Nairobi, 2013.
[11] Internet World Stats, (2018, Dec, 31). Internet Penetration in Africa [Online]. Available https://www.internetworldstats.com/stats1.htm.
[12] A.A, Oni, and C.K. Ayo. An empirical investigation of the level of users' acceptance of e- banking in Nigeria. J. Internet Bank. Commer.Vol. 15, pp. 1–13, 2010.
[13] Central Bank of Nigeria (CBN). Guidelines on Electronic Banking in Nigeria [Online]. Available.https://www.arca.network/lib/E-BANKING-Regulation-document. 2003.
[14] O.R. Ehimen, and A. Bola. Cybercrime in Nigeria. Bus. Intell. J. 3 (1), pp. 93–98, 2010.
[15] A. Odunfa. Nigeria: Report on Cyber Threat Calls for Quick Passage of 2012 Bill [Online]. Available.http://www.allafrica.com/stories/201405080279.Html, 2014.
[16] Ponemon Institute. The Impact of Data Breaches on Reputation & Share Value.Available.
[17] B.A. Omodunbi, P.O. Odiase, O.M. Olaniyan, and A.O. Esan. Cybercrimes in Nigeria: analysis, detection and prevention. FUOYE J. Eng. Technol. 1 (1), pp. 37–42, 2016.
[18] E. Dunkley (2017, Mar, 13). A Tale of Two Cyber Bank Heists that Reveals Their Vulnerability.Financial Times Retrieved from. https://www.ft.com/content/2bc83132- e18-11e6-ba01-119a44939bb6?mhq5j=e3.
[19] A.J. Ebenezer, A.M. Paula, and T.Allo.Risk and investment decision making in the technological age: a dialysis of cyber fraud complication in Nigeria. Int. J. Cyber, 2016.
[20] U.A. Ojedokun, and M.C. Eraye. Socioeconomic lifestyles of the yahoo-boys: a study of perceptions of university students in Nigeria. Int. J. Cyber Criminol. 6 (2), pp. 1001– 1013, 2012.
[21] M. Lagazio, N.Sherif, and M. Cushman. A multi-level approach to understanding the impact of cybercrime on the financial sector. Comput. Secur.Vol. 45, pp. 58–74, 2014.
[22] Z. Mohammed. NITDA Raises Alarm over Potential Cyber Attacks to Banks. Govt Agencies, Others (Online) Available. https://www.nigerianews.net/nitda-raisesalarm-,2018.
[23] O.J. Olayemi. A socio-technological analysis of cybercrime and cyber security in Nigeria. Int. J. Sociol. Anthropol. 6 (3), pp. 116–125, 2014.
[24] B.A. Omodunbi P.O. Odiase, O.M. Olaniyan, and A.O. Esan. Cybercrimes in Nigeria: analysis, detection and prevention. FUOYE J. Eng. Technol. 1 (1), pp. 37–42, 2016.
[25] KPMG, 2017. How can Nigerian banks start to improve internet banking penetration?.
[26] Rahul kumar and Dr.abhineet anand " Internet Banking System & Security Analysis" International Journal of Engineering And Computer Science ISSN:2319-7242 Volume 6 Issue 4 April 2017.
[27] "Md Hamid Uddin and Md Hakim Ali Taylor's and M. Kabir Hassan" Cybersecurity Hazard and Financial System Vulnerability: A synthesis of literature This copy at SSRN is the preprint version. The published version is available at https://link.springer.com/article/10.1057/s41283-020-00063-2.
[28] "Petrit Hasanaj1 & Beke Kuqi2", Analysis of Financial Statements: The Importance of Financial Indicators in Enterprise Email: petrithasanaj gmail.com Received: May 20, 2019; Accepted: June 1, 2019; Published: June 19, 2019.
[29] Ashwini Sheth1 , Mr. Schain Bhosale2 , Mr. Famish Kurupkar" Research Paper On Cyber Securitycontemporary Research In India (Issn 2231-2137): Special Issue : April, 2021.
[30] Muhammad Baqir on 10 June 2021. SWIFT Network And Maintenance Of Its Cybersecurity In The Era Of Global Digitization Ross, R.; R. Groubert; D. Bordeaux; R. McQuaid; Systems Security Engineering, SP 800-160 volume 2, National Institute of Standards and Technology, USA, March 2018, https://csrc.nist. gov/CSRC/media/Publications/sp/800 160/ vol2/draft/documents/sp800-160-vol2-draft.pdf.
[31] S. M. Ikhtiar Alam, Ph.D. What is SWIFT in International Banking, Jahangir nagar University, Bangladesh Corresponding Author: ikhtiar@juiv.edu.
[32] Susan Scott, John Van Reenen and Markos Zachariadis, The Impact of the Diffusion of a Financial Innovation on Company Performance: An Analysis of SWIFT Adoption 2010.
[33] Markos Zachariadis, Susan V. Scott The Society for Worldwide Interbank Financial Telecommunication (SWIFT).

Cite this article as: Neetu Rani Sharma, Harshita Kamboj, S.K. Gupta, Security analysis of swift financial software, International Journal of Research in Engineering and Innovation Vol-6, Issue-5 (2022), 327-337. *https://doi.org/10.36037/IJREI.2022.6505*.