e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 7, July 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707216 |

Files Sharing using Two Factor Authentication

Rajesh N, Keerthan P U

Assistant Professor, Department of MCA, AMC Engineering College, Bengaluru, India

Student, Department of MCA, AMC Engineering College, Bengaluru, India

ABSTARCT: In the digital age, file sharing has become a fundamental aspect of both personal and professional communication. However, the security of shared files is often compromised, leading to significant data breaches and unauthorized access. This research paper explores an enhanced file-sharing system that incorporates two-factor authentication (2FA) to bolster security measures. By requiring users to verify their identity through a combination of something they know (password) and something they have (mobile device or hardware token), this method ensures a more robust defense against unauthorized access. The study delves into various 2FA techniques, evaluates their effectiveness in safeguarding sensitive information, and examines user adoption and convenience. The proposed solution aims to provide a comprehensive and secure framework for file sharing that mitigates risks associated with traditional single-factor authentication methods. Through theoretical analysis and practical implementation, this research highlights the critical role of 2FA in enhancing the security of digital file-sharing systems.

I. INTRODUCTION

Today security concerns are on the rise in all areas such as banks, governmental applications, healthcare industry, military organization, educational institutions, etc. Government organizations are setting standards, passing laws, and forcing organizations and agencies to comply with these standards with non-compliance being met with wide-ranging consequences. There are several issues when it comes to security concerns in these numerous and varying industries with one common weak link being passwords. Most systems today rely on static passwords to verify the user's identity. However, such passwords come with major management security concerns. Users tend to use easy-to-guess passwords, use the same password in multiple accounts, write the passwords or store them on their machines, etc. Furthermore, hackers have the option of using many techniques to steal passwords such as shoulder surfing, snooping, sniffing, guessing, etc. Several 'proper' strategies for using passwords have been proposed. Some of which are very difficult to use and others might not meet the company's security concerns. Two factor authentication using devices such as tokens and ATM cards have been proposed to solve the password problem and have shown to be difficult to hack. Two factor authentication also have disadvantages which include the cost of purchasing, issuing, and managing the tokens or cards. From the customer's point of view, using more than one two-factor authentication system requires carrying multiple tokens/cards which are likely to get lost or stolen. Mobile phones have traditionally been regarded as a tool for making phone calls. But today, given the advances in hardware and software, mobile phones use has been expanded to send messages, check emails, store contacts, etc. Mobile connectivity options have also increased. After standard GSM connections, mobile phones now have 2 infra-red, Bluetooth, 3G, and WLAN connectivity. Most of us, if not all of us, carry mobile phones for communication purpose. Several mobile banking services available take advantage of the improving capabilities of mobile devices. From being able to receive information on account balances in the form of SMS messages to using WAP and Java together with GPRS to allow fund transfers between accounts, stock trading, and confirmation of direct payments via the phone's micro browser. Installing both vendor-specific and third-party applications allow mobile phones to provide expanded new services other than communication. Consequently, using the mobile phone as a token will make it easier for the customer to deal with multiple two factor authentication systems; in addition, it will reduce the cost of manufacturing, distributing, and maintaining millions of tokens. In this paper, we propose and develop a complete two factor authentication system using mobile phones instead of tokens or cards. The system consists of a server connected to a GSM modem and a mobile phone client running a J2ME application. Two modes of operation are available for the users based on their preference and constraints. The first is a stand-alone approach that is easy to use, secure, and cheap. The second approach is an SMS-based approach that is also easy to use and secure, but more expensive. The system has been implemented and tested.

II. LITERATURE SURVEY

By definition, authentication is the use of one or more mechanisms to prove that you are who you claim to be. Once the identity of the human or machine is validated, access is granted. Authentication is generally required to access secure

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

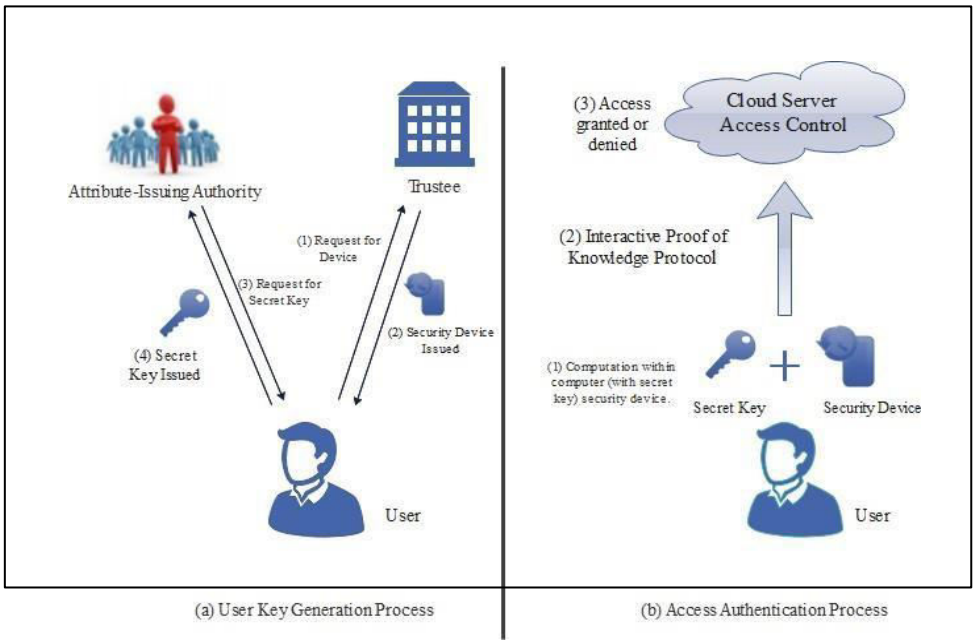
| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707216 |

data or enter a secure area. The requestor for access or entry shall authenticate himself based on proving authentically his identity by means of What the requestor individually knows as a secret, such as a password or a Personal Identification Number (PIN), or What the requesting owner uniquely has, such as a passport, physical token, or an ID-card, or What the requesting bearer individually is, such as biometric data, like a fingerprint or the face geometry. Two-factor authentication means using any independent two of these authentication methods (e.g. password + value from physical token) to increase the assurance that the bearer has been authorized to access secure systems. The owner of secure data or the operator of such secure systems is implementing two-factor authentication for laptops first because of the inherent security risks in mobile computers, to make it more difficult for unauthorized persons to use a "found" laptop to access secure data or systems. With mobile phones or smart phones, the quality of the problem does not change: A lost or left phone shall not be activated to enable the finder for unauthorized access to secure data or system. Multi-factor authentication hence means two or more of the authentication factors required for being authenticated.

Three universally recognized authentication factors exist today: what you know (e.g. passwords), what you have (e.g. ATM card or tokens), and what you are (e.g. biometrics). Recent work has been done in trying 5 alternative factors such as a fourth factor, e.g. somebody you know, which is based on the notion of vouching. Two factor authentications is a mechanism which implements two of the above mentioned factors and is therefore considered stronger and more secure than the traditionally implemented one factor authentication system. Withdrawing money from an ATM machine utilizes two factor authentication; the user must possess the ATM card, i.e. what you have, and must know a unique personal identification number (PIN), i.e. what you know. Passwords are known to be one of the easiest targets of hackers. Therefore, most organizations are looking for more secure methods to protect their customers and employees. Biometrics are known to be very secure and are used in special organizations, but they are not used much in secure online transactions or ATM machines given the expensive hardware that is needed to identify the subject and the maintenance costs, etc. Instead, banks and companies are using tokens as a mean of two factor authentication.

A security token is a physical device that an authorized user of computer services is given to aid in authentication. It is also referred toas an authentication token or a cryptographic token. Tokens come in two formats: hardware and software. Hardware tokens are small devices which are small and can be conveniently carried. Some of these tokens store cryptographic keys or biometric data, while others display a PIN that changes with time. At any particular time when a user wishes to log-in, i.e. authenticate, he uses the PIN displayed on the token in addition tohis normal account password. Software tokens are programs that run on computers and provide a PIN that changes with time. Such programs implement a One Time Password (OTP) algorithm. OTP algorithms are critical to the security of systems employing them since unauthorized users should not be able to guess the next password in the sequence. The sequence should be random to the maximum possible extent, unpredictable, and irreversible.



Factors that can be used in OTP 6 generation include names, time, seed, etc. Several commercial two factor authentication systems exist today such as BestBuy's Betoken, RSA'sSecurID, and Secure Computing's

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707216 |

Safeword.BesToken applies two-factor authentication through a smart card chip integrated USB token. It has a great deal of functionality by being able to both generate and store users' information such as passwords, certificates and keys. One application is to use it to log into laptops. In this case, the user has to enter a password while the USB token is plugged to the laptop at the time of the login.

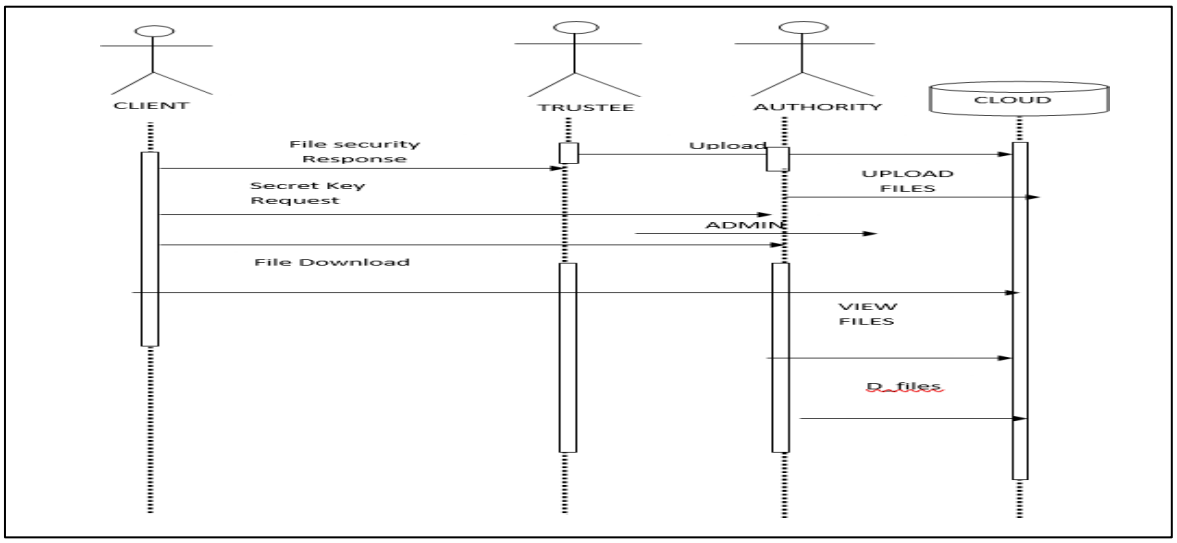
III. PROBLEM DEFINITION

A hacker must compromise both the USB and the user account password to log into the laptop. SecurID from RSA uses a token (which could be hardware or software) whose internal clock is synchronized with the main server. Each token has a unique seed which is used to generate a pseudo-random number. This seed is loaded into the server upon purchase of the token and used to identify the user. An OTP is generated using the token every 60 seconds. The same process occurs at the server side. A user uses the OTP along with a PIN which only he knows to authenticate and is validated at the server side. If the OTP and PIN match, the user is authenticated. In services such as ecommerce, a great deal of time and money is put into countering possible threats and it has been pointed out that both the client and the server as well as the channel of communication between them are imperative.In 2005 the National Bank of Abu Dhabi (NBAD) became the first bank in the Middle East to implement two factor authentication using tokens. It employed the RSA SecurID solution and issued its 19000 customers small hardware tokens. The National Bank of Dubai (NBD) made it compulsory for commercial customers to obtain tokens; as for personal customers the bank offered them the option to obtain the tokens. In 2005, Bank of America also began providing two factor authentication for its 14 million customers by offering hardware tokens. Many international banks also opted to provide their users with tokens for additional security, such as Bank of Queensland, the Commonwealth Bank of Australia and the Bank of Ireland. Using tokens involves several steps including registration of users, token production and distribution, user and token authentication, and user and token revocation among others. While tokens provide a much safer environment for users, it can be very costly for organizations. For example, a bank with a million customers will have to purchase, install, and maintain a million tokens. Furthermore, the bank has to provide continuous support for training customers on how to use the tokens. The banks have to also be ready to provide replacements if a token breaks or gets stolen. Replacing a token is a lot more expensive than replacing an ATM card or resetting a password. From the customer's prospective, having an account with more than one bank means the need to carry and maintain several tokens which constitute a big inconvenience and can lead to tokens being lost, stolen, or broken. In many cases, the customers are charged for each token. We propose a mobile-based software token that will save the organizations the cost of purchasing and maintaining the hardware tokens. Furthermore, will allow customers to install multiple software tokens on their mobile phones. Hence, they will only worry about their mobile phones instead of worrying about several hardware tokens.

IV. HARDWARE & SOFTWARE REQUIREMENT

Hardware:

1.Processor: Pentium 4.



| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707216 |

2.RAM: 512 MB or more.
3.Hard disk: 16 GB or more.
4.GSM modem.
Software:
1.NetBeans 6 and above.
2.JDK 6 and above.
3.Sun Wireless toolkit for J2ME.

V. IMPLEMENTATION

Client Design A J2ME program is developed and installed on the mobile phone to generate the OTP. The program has an easy to-use GUI that is developed using the NetBeans drag and drop interface. The program can run on any J2ME-enabled mobile phone. The OTP program has the option of (1) generating the OTP locally using the mobile credentials. e.g. IMEI, or (2) requesting the OTP from the server via an SMS message. The default option is the first method which is cheaper since no SMS messages are exchanged between the client and the server.

However, the user has the option to select the SMS-based method. In 22 order for the user to run the OTP program, the user must enter his username and PIN and select the OTP generation method. The username, PIN, and generated OTP are never stored on the mobile phone.

Database Design A database is needed on the server side to store the client's identification information such as the first name, last name, username, pin, password, mobile IMEI number, unique symmetric key, and the mobile telephone number for each user. The password field will store of the 10 minute password. It will not store the password itself. Should the database be compromised the hashes cannot be reversed in order to get the passwords used to generate those hashes. Hence, the OTP algorithm will not be traced. Server Design A server is implemented to generate the OTP on the organization's side. The server consists of a database as described in Section 3.C and is connected to a GSM modem for SMS messages exchange. The server application is multithreaded. The first thread is responsible for initializing the database and SMS modem, and listening on the modem for client requests. The second thread is responsible for verifying the SMS information, and generating and sending the OTP.

A third thread is used to compare the OTP to the one retrieved using the connection-less method. In order to setup the database, the client must register in person at the organization. The client's mobile phone/SIM card identification factors, e.g. IMEI, are retrieved and stored in the database, in addition to the username and PIN. The J2ME OTP generating software is installed on the mobile phone. The software is configured to connect to the server's GSM modem in case the SMS option is used. A unique symmetric key is also generated and installed on both the mobile phone and server. Both parties are ready to generate the OTP at that point.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com