Special Issue on Proceedings of International Conference on Newer Trends and Innovation in Nanotechnology, Materials Science, Science and Technology March 2021. International Journal of Aquatic Science, Vol 12, Issue

FRAMEWORK TO SECURE DATA BYMULTI LAYERED AUTHENTICATION

[1*]**M. Jebakumari,***Assistant Professor, CSE Department, Nehru Institute of Technology*

[2]*Beaulah David, Assistant Professor, CSE Department, Nehru Institute of Technology*

[*]*Correspondent e-mail:*nitjebakumari@nehrucolleges.com

Abstract- Authenticated key exchange (AKE) is one of the most important applications in applied cryptography, where a user interacts with a server to set up a session key where pre-registered information (aka. authentication factor), such as a password or biometrics, of the user is stored. While single-factor AKE is widely used in practice, higher security concerns call for multi-factor AKE (MFAKE) schemes, e.g. combining both passwords and biometrics and device simultaneously. However, in some casually designed schemes, security is even weakened in the sense that leakage of one authentication factor will defeat the whole MFAKE protocol. Furthermore, an inevitable by-product arises that the usability of the protocol often drops greatly. To summarize, the existing multi-factor protocols did not provide enough security and efficiency simultaneously. Here, we make one step ahead by proposing a very efficient MFAKE protocol. We define the security model and give the according security analysis. We also implement our proposed method as textual, graphical, biometric and device password to access the user accounts. The theoretic comparisons and the experimental results show that our scheme achieves both security and usability.

Keywords: Authenticated key exchange, session key.

I .Introduction

NETWORK SECURITY

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Only network security can remove Trojan horse viruses if it is activated. Network security involves the authorization of access to data in a network, which is controlled by the network administrator.

DOTNET

Microsoft .net is a set of micro soft software technologies for rapidly building and integrating xml web services, micro soft windows-based applications, and web solutions. The .net framework is a language-neutral platform for writing programs that can easily and securely interoperate. There's no language barrier with .net: there are numerous languages available to the developer including managed C++, C#, visual basic and java script.

SQL SERVER 2005

SQL Server 2005 is the successor to SQL Server 2000. It included native support for managing XML data, in addition to relational data. For this purpose, it defined an xml data type that could be used either as a data type in database columns or as literals in queries. XML columns can be associated with XSD schemas. XML data being stored is verified against the schema. XML is

converted to an internal binary data type before being stored in the database.

User authentication is a very important part for many information systems. In practice, it is often done via the following methods:

- **Password-Based Authentication:** it is the most popular way, while quite insecure in some cases. E.g., in the Worst Password List compiled by Splash Data (among 3.3 million passwords used for test, almost 20,000 were in fact"123456"). The statistics show that most passwords in use are not so hard to guess.

- **Hardware-Based Authentication:** With storage space for long secret keys and computation power for authentication, hardware provides higher security than password. But if it was stolen or lost, which happens in daily life occasionally, the authentication fails completely.

- **Biometrics-Based Authentication:** Utilizes the unique and life-long invariant property of the biometrics. But it is not so reliable, e.g., biometric characteristics such as fingerprint can be easily "copied" without the awareness of the owner.

Single-factor authentication only provides limited security, then combining these methods together is considered as a good way to achieve higher security. But, in fact, many exiting multi-factor authentication schemes are quite insecure.

This again, raised the need for secure multi-factor authentication schemes. In general, there are several issues should be addressed by multi-factor authentication schemes:

- **Efficiency:** Complex protocol design should be avoided, which may cause expensive computation and communication costs. In practice, a device with high computation power is usually not cheap, and heavy bandwidth occupation due to authentication will make an information system unsalable, and vulnerable to DoS attacks.
- **Robustness:** Whenever there is one factor uncorrupted, the authentication scheme should remain secure, which is a basic security requirement for multi-factor authentication. But many existing schemes could not meet it: e.g., using redundant authentication, even worse, introducing more weakness.
- **Privacy:** Biometric characteristics are acknowledged as one kind of privacy information, so which must be protected to avoid leakage. In addition, the leakage of biometric will not only break the security in the authentication, but also can lead to further social damage.
- **Session Key Agreement:** Authentication is just a way to prevent illegal users from entering a system. While the subsequent communications also need to be protected. So it is ideal to set up a session key between the client and server by the end of an authentication.

- **Usability:** The participation of people requires the authentication schemes are friendly to use: e.g., most people cannot remember long and random passwords, and hate to carry many different devices; even taking long and random enough

passwords and more different devices can improve the security.

II. Related Works

Emilia no De Cristofaro,Honglu Du, Julien Freudiger, Greg Norcie (2014) proposed a two-factor authentication (2F) aims to enhance resilience of password-based authentication by requiring users to provide an additional authentication factor, e.g., a code generated by a security token. It also introduces non-negligible costs for service providers and requires users to carry out additional actions during the authentication process. In that paper, they presented an exploratory comparative study of the usability of 2F technologies. First, they conduct a pre-study interview to identify popular technologies as well as contexts and motivations in which they are used.

They then present the results of a quantitative study based on a survey completed by 219 Mechanical Turk users, aiming to measure the usability of three popular 2F solutions: codes generated by security tokens, one-time PIN received via email or SMS, and dedicated Smartphone apps (e.g., Google Authenticator). They record contexts and motivations, and study their impact on perceived usability. They find that 2F technologies are overall perceived as usable, regardless of motivation and/or context of use. They also present an exploratory factor analysis, highlighting that three metrics – ease-of-use, required cognitive efforts, and trustworthiness – are enough to capture key factors affecting 2F usability.

FadiAloul, Syed Zahidi, Wasim El-Hajj (2009) proposed a technique for executing two factor authentication utilizing cell phones. The proposed strategy guarantees that validating to administrations, for example, web based saving money or ATM machines, is done in an exceptionally secure way. The proposed framework involves using a cell phone as a product token for One Time Password generation. The produced One Time Password is substantial for just a short user-defined time frame and is created by factors that are unique to both, the client and the cell phone itself. Moreover, a SMS-based instrument is actualized as both a reinforcement system for retrieving the secret word and as a conceivable mean of synchronization. The proposed strategy has been executed and tried. Introductory results demonstrate the accomplishment of the proposed technique.

AleksandrOmetov, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, TommiMikkonen and YevgeniKoucheryavy (2017) proposed a work reveals insight into the development of verification frameworks towards Multi-Factor Authentication (MFA) beginning from Single-Factor Authentication (SFA) and through Two-Factor Authentication (2FA). Especially, MFA is required to be used for human-to-everything connections by empowering quick, easy to understand, and dependable verification while getting to an administration.

That paper reviews the effectively accessible and developing sensors (factor suppliers) that consider confirming a client with the framework specifically or by including the cloud. The comparing challenges from the client and also the specialist organisation viewpoint are likewise investigated. The MFA framework in view of turned around Lagrange polynomial inside Shamir's Secret Sharing (SSS) plot is additionally proposed to empower more adaptable verification. This arrangement covers the instances of verifying the client regardless of whether a portion of the elements are bungled or missing. Our structure takes into consideration qualifying the missing

elements by confirming the client without revealing delicate biometric information to the check element.

The idea proposed by Asif Amin et al., (2017) was about two factor authentication which was to overcome the single factor confirmation, e.g. passwords, was no more analyzed as secure in the World Wide Web. That has never been less troublesome in Securing the framework and remote access. Straightforward, clear and simple to-figure passwords, for example, names and age, are easily discovered through mechanized mystery key social affair programs. The security and protection dangers through malware are dependably always becoming both in amount and in addition quality. Extended access to data expands shortcoming to hacking, splitting of passwords and online cheats.

In that affiliation the ordinary login/secret key validation was considered insufficiently secure for a few security-basic applications, for example, login to Mailing Accounts, Social Networks, Gadgets, Financial records, official secured systems, business sites online and so forth. Obliging in excess of one free factor builds the trouble of giving false accreditations. Two-factor verification proposition ensure a higher assurance level by expanding the single confirmation factor. That paper centers around the execution of two-factor confirmation techniques by utilizing the two clients benevolent customary Alphanumeric Password and graphical Password as entryway for validation. In this paper they had depicted that the two factor Authentication framework plan and outline execution. Hence bearing an extra watchword includes an additional layer of security.

Two Factor Authentication (2017) by Asif Amin, IsrarulHaq, MonisaNazir the ideas of D.F.L. Souza et al., (2017) was the client verification in view of multi factor approach is introduced. For that security procedure, a client validates into a framework utilizing an arrangement of three attributes identified with physical, ownership and information factors. Biometrics confirmation speaks to the physical factor. An optical validation strategy in light of two-bar obstruction and clamorous maps finish the proposed plot. In that sense, the seed of a disorderly guide speaks to a client watchword comparing to a learning factor and a resultant interferogram from an optical validation procedure speaks to the ownership factor. Numerical reenactment exhibits the plausibility of our technique. Also, they perform key space and measurable examination to exhibit the viability of the arrangement.

A Multi Factor Authentication Approach Based on Biometrics, Optical Interference and Chaotic MapsD(2017) by F. L. Souza, A. M. F. Burlamaqui and G. L. Souza Filho.The work done by S.Vaithya Subramanian et al., (2017) detailed about the present advanced day with wonderful improvement in Computer area, Single factor validation, e.g. passwords, was no more inspected as secure in the World Wide Web. It had never been less troublesome in Securing the framework and remote access. Straightforward, evident and simple to-figure passwords, for example, names and age, are easily discovered by means of modernized mystery key social occasion programs. The security and protection dangers through malware are dependably continually becoming both in amount and in addition quality.

Extended access to data expands shortcoming to hacking, splitting of passwords and online fakes. In that affiliation the ordinary login/secret word verification was considered deficiently secure for a few security-basic applications, for example, login to Mailing Accounts, Social Networks, Gadgets, Financial records, official secured systems, business sites online and so forth. Obliging in excess of one free factor expands the trouble of giving false qualifications. Two-

factor confirmation proposition ensure a higher insurance level by expanding the single validation factor.

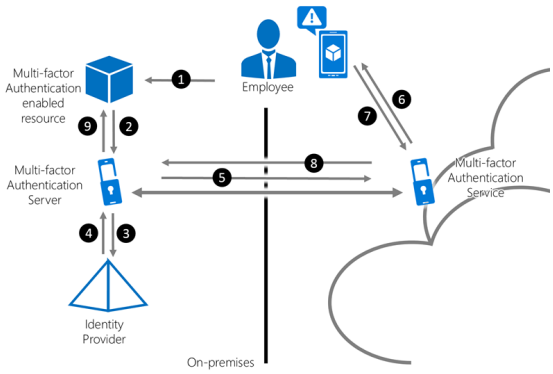
This paper centers around the execution of two-factor verification strategies by utilizing the two clients inviting customary Alphanumeric Password and graphical Password as passage for validation. An endeavor has been made by utilizing two factors Authentication, and in this paper we portray the two factor Authentication framework plan and outline usage. Subsequently bearing an extra secret key includes an additional layer of security.

Two Factor Authentications For Secured Login In Support Of Effective Information Preservation And Network Security (2017) By S. Vaithyasubramanian1, A. Christy1 and D. Saravanan2 1Sathyabama University, Chennai, India.The paper by Xini Huang et al., (2011) deciphers a major aspect of the security inside disseminated frameworks, different administrations and assets require assurance from unapproved utilize.

Remote verification was the most normally utilized technique to decide the character of a remote customer. That paper explores an efficient approach for validating customers by three components, in particular watchword, keen card, and biometrics. A nonexclusive and secure structure was proposed to update two-factor validation to three-factor confirmation. The change not just essentially enhances the data confirmation requiring little to no effort yet in addition secures customer protection in circulated frameworks. Moreover, their system holds a few practice-accommodating properties of the hidden two-factor confirmation, which they accept is of free intrigue.

A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems(2011) By Xinyi Huang, Yang Xiang, Member, IEEE, Ashley Chonka,Jianying Zhou, and Robert H. Deng, Senior Member, IEEE

III. System Approach



This step is used to login the individual sender and receiver. It creates a graphical password that is used for the login purpose of the sender and receiver. This graphical password is created by using the information's about the sender and receiver and with the help of sessions using in it. These passwords are accessed only in the particular location of the secured image.

These graphical passwords are used to increase the authentication to the data. The graphical password is generated based on the users clicking point which is based on the corresponding **x** axis and **y** axis value. If the values of the clicking point match with the registered value, then only he can login and process this system.

Biometric Password Authentication

The step is used to generate the biometrics scheme for the authenticated data. Registered finger print value is checked with the current fingerprint of the person who tries to login. The biometrics of both the sender and receiver is scanned for increasing their privacy. This is done by checking pixel by pixel of the registered fingerprint and current user fingerprint..By using this biometrics the data is being prevented. The sender and receiver perform the data transaction by using biometrics scheme. So the system is full secured.

Hardware-Based Authentication
With storage space for long secret keys and **Feasibility Study**

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

The feasibility study investigates the problem and the information needs of the stakeholders. It seeks to determine the resources required to provide an information systems solution, the cost and benefits of such a solution, and the feasibility of such a solution. The analyst conducting the study gathers information using a variety of methods, the most popular of which are:

- Interviewing users, employees, managers, and customers.
- Developing and administering questionnaires to interested stakeholders, such as potential users of the information system.
- Observing or monitoring users of the current system to determine their needs as well as their satisfaction and dissatisfaction with the current system.
- Collecting, examining, and analyzing documents, reports, layouts, procedures, manuals, and any other documentation relating to the operations of the current system.
- Modeling, observing, and simulating the work activities of the current system.

The goal of the feasibility study is to consider alternative information systems solutions, evaluate their feasibility, and propose the alternative most suitable to the organization. The feasibility of a proposed solution is evaluated in terms of its components. These components are:

- Economical feasibility
- Technical feasibility
- Social feasibility
- Operational feasibility

Economical Feasibility

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

Technical Feasibility

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

Social Feasibility

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity.

The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

Operational Feasibility

The ability, desire, and willingness of the stakeholders to use, support, and operate the proposed computer information system. The stakeholders include management, employees, customers, and suppliers. The stakeholders are interested in systems that are easy to operate, make few, if any, errors, produce the desired information, and fall within the objectives of the organization.

IV. Implementation

Textual Authentication

The User Registration has both the sender and receiver registration process. Initially they have to register for their interaction between them. The sender and receiver registered by using the individual textual passwords. The Registration process is common for both the sender and receiver.

During the registration phase the user have to register the graphical password and their finger print. These registered values are stored in database for security verification purposes while the login process.

Graphical Password Generationcomputation power for authentication, hardware provides higher security than password. But if it was stolen or lost, which happens in daily life occasionally, the authentication fails completely.

Data Send

After the multifactor authentication the sender begins to send the data. The sender sends the data to the receiver in the encryption format for the security purpose. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

The encryption process is done by AES algorithm. The data's are encrypted so the unknown person can't access the files which are sent by sender. These encryptions are known only by the authorized sender. AES is considered one of the most efficient algorithms currently available.

Data Receive

After the sender sends the data the receiver access the data using the session password. Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. After finishing multifactor authentication the receiver can decrypt and view the original format of the data which has sent by the sender. Authorized person can only decrypt the file using the key.

VI. References

[1] AleksandrOmetov ., Sergey Bezzateev ., Niko Mäkitalo., Sergey Andreev., TommiMikkonen., and YevgeniKoucheryavy., (2017) "Multi-Factor Authentication: A Survey, Cryptography" MDPI AG,Basel,Switzerland, http://creativecommons.org/licenses/by/4.0/

[2] Asif Amin., IsrarulHaq., and MonisaNazir., (2017) "TWO FACTOR AUTHENTICATION" IJCSMC,Vol. 6, Issue. 7, pp. 5-8.

[3] D. F. L. Souza., A. M. F. Burlamaqui., and G. L. Souza Filho (2017) "A Multi Factor Authentication Approach Based on Biometrics, Optical Interference and Chaotic Maps" vol. 15, pp. 1700-1708.

[4] Emiliano De Cristofaro., Honglu Du PARC., Julien Freudiger PARC., and GregNorcie (2014) "A Comparative Usability Study of Two-Factor Authentication", in USEC

[5]Caspar.F, Berger.T, and Hautle.I, (2004) "The right view of your patient: A computer assisted, individualized module for psychotherapy training," Psychotherapy: Theory, Research, Practice, Training, vol. 41, no. 2, pp. 125–135.

[6]Liao K.P, Cai.T, Gainer.V, Goryachev.S, Zeng-treitler.S, Raychaudhuri.S, Szolovits.P, Churchill.S, Murphy.S, Kohane et al.I.,(2010) "Electronic medical records for discovery research in rheumatoid arthritis," Arthritis care & research, vol. 62, no. 8, pp. 1120–1127.

[7]Lehman L.W, Saeed.M, Long.W, Lee.J, and Mark.R, (2012) "Risk stratification of icu patients using topic models inferred from unstructured progress notes," in AMIA Annual Symposium Proceedings, vol.12. American Medical Informatics Association, p. 505

[8]Luo.Y, Sohani. A. R, Hochberg E. P, and Szolovits.P, (2014) "Automatic lymphoma classification with sentence subgraph mining from pathology reports," Journal of the American Medical Informatics Association, vol. 21, no. 5, pp. 824–832.

[9]Pestian.J., Nasrallah.H, Matykiewicz.P, Bennett.A, and Leenaars.A, (2010) "Suicide note classification using natural language processing: A content analysis," Biomedical informatics insights, vol. no. 3, p. 19.

[10]Rude.S, Gortner E.-M, and Pennebaker.J, (2004) "Language use of depressed and depression-vulnerable college students," Cognition & Emotion, vol. 18, no. 8, pp. 1121–1133.

[11]Schulz.A, Stolz.T, and Berger.T, (2014) "Internet-based individually versus group guided self-help treatment for social anxiety disorder: protocol of a randomized controlled trial," BMC psychiatry, vol. 14, no. 1, p. 115.

[12]Stangier.U., Heidenreich.T, Berardi.A, Golbs.U, and Hoyer.J, (1999) "Die erfassungsozialerphobiedurch die social interaction anxiety scale (sias) und die social phobia scale (sps)," Z KlinPsycholPsychiatrPsychother, vol. 28, pp. 28–36.

[13]Savova.G. K , Masanz J. J, Ogren P. V, Zheng.J, Sohn.S, KipperSchuler. K. C., and Chute C. G, (2010) "Mayo clinical text analysis and knowledge extraction system (ctakes): architecture, component evaluation and applications," Journal of the American Medical Informatics Association, vol. 17, no. 5, pp. 507–513.

[14]Tausczik.Y. R., and Pennebaker J. W,(2010) "The psychological meaning of words: Liwc and computerized text analysis methods," Journal of language and social psychology, vol. 29, no. 1, pp. 24–54.

[15]Van der Zanden.R., Curie.K,. Van Londen.M, Kramer.J, Steen.G, and Cuijpers.P, (2014) "Web-based depression treatment: Associations of clients? word use with adherence and outcome," Journal of affective disorders, vol. 160, pp. 10–13.

[16] Fadi A Aloul., Syed Zahidi., and Wasim El-Hajj (2009) "Multi Factor Authentication Using Mobile Phones" in International Journal of Mathematics and Computer Science, 4(2009), no.2, 65-80.

[17] S. Vaithyasubramanian ., A. Christy., and D. Saravanan., (2015) "TWO FACTOR AUTHENTICATIONS FOR SECURED LOGIN IN SUPPORT OF EFFECTIVE INFORMATION PRESERVATION AND NETWORK SECURITY" (2017) Vol. 10, No.5 , March 2015.

[18] Xinyi Huang., Yang., (2011) "A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems" vol.22, pp.1390-1397.