A Survey on: Continues and Transparent User Identity verification for secure internet Services

Sreedhar Kumar S[1] . Hemaswetha L P[2] . Rajshanker Gobbi[3]

[1]Dr. T. Thimmaiah Institute of Technology, VTU, KGF, India
[2]New Horizon College of Engineering, Bengaluru, India.
[3]Indian Institute of Technology, Dharwad, India

Received: 30 March 2022 / Revised: 25 April 2022 / Published Online: 12 June 2022

Abstract – A session browsing in internet is trivially under a specific username and password. Each session lasts for a defined time with a conditional monitoring system of the same. In this paper is brief study is made on how these session are monitored, conditions applied to grant a excess session time and then finally preset an overview discussion on these schemes and techniques under modern devices such as PC's and Smart Phones.

Index Terms – Conditional monitoring, Secure Internet Browsing, Session Timeout

---

I. INTRODUCTION

We today have imbedded internet into our daily life as much as we cannot observe an activity in its absence. Currently 87% of internet authentication is done with a unique username and password and there by the access to session is granted[1][14]. This step basically does not contain any future checksums. Security in modern day web environment has become a concern to researches and developers as the frequency of cybercrime and malfunctionalities has seen a hike.

In order to maintain the security levels many biometric algorithms and techniques has been proposed under finger print analysis and face detection, among which a major focus is drawn with finger print. Still based on these observations, a remarkable security enhancement is been made, but a guarantee on making the same is still a concern.

In major sectors like banking and e-commerce, section time is considered a valuable asset to determine the quality of resources utilized. As once an authentic logic is seen, the current system grants the usage of resources and thus often public environmental data accessing has seen a thread. In this paper, a cashma scheme and other beneficiary schemes has been discussed.

II. LITERATURE REVIEWS

From few selective papers and research articles the following review is been done, the major objective of this paper is to summarize various schemes, models and protocols under secure internet domain. Various schemes of verifications has been proposed and are classified as continues verification and transparent verification. Under continues verification the proposed for the systems under a session timeout and are conditionally verified with an authentic username and password.

Under the second scheme, the data is processed and monitored in backend and a best example for this is Gmail session. This is an auto-reliving session and requires manual logout.

A. CASHMA Scheme

Context aware security by hierarchical multilevel architecture (CASHMA) [1] is a proposed system for a secure web services under various threading scenarios. This scheme implements the data transfer in a secure and reliable manner for e-commerce and banking applications. This scheme has a high impact factor and can be used to replace the previous models. In our contribution, we focus on CASHMA scheme limitations and enhancements for better performance and reliability. Generally, CASHMA is a continuously verifying protocol under a session time out mechanism.

CASHMA scheme has [3][6] basic references of logic from the paper with a major focus towards continues authentication of the session and maintain reloggin parametics on the same device. The multi-model biometric authentication feature is been shown a high focus in this paper and in [9].

B. Security Assessment

As seen in A, Security assessment also plays an important role in verifying and validating the system security model. This has a model-based quantitative security assessment. This terminology is seen widely since late 1980's with a theoretical formulations and qualitative analysis. The current CASHMA has features to align with file directories and subsystem under web environment. The ability to perform ad-hoc is also its main focus.

III. CASHMA REVIEWS AND PROTOTYPING

CASHMA has a novelty in its features of securing and dealing with web services. *Architecture*: The CASHMA protocol consists of a mixed model under web services with a dedicated user authentication unit. Each time a session is initiated, the CASHMA authentication unit is activated with and thus a verification in an continues manner is done.

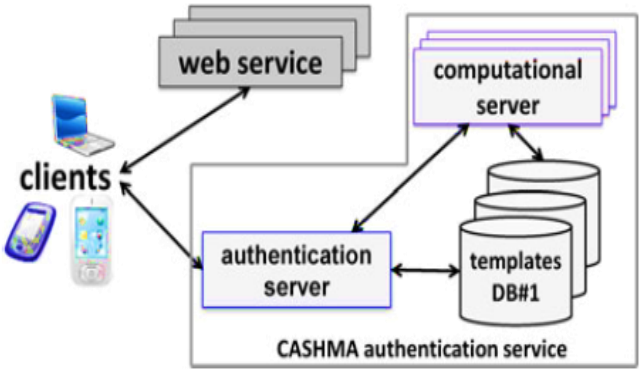

Fig 1: CASHAM Architecture

CASHMA scheme reduces the burden of data transferring and also minimizes raw data flow from base devices to serve. The major legal bailments are also counted in the overall system design. Since continues authentication is independent of the platform and environment, CASHMA scheme can work in different template and provides a verified certificate for the certified users under these untrusted web domain services for trust based services and transmissions.

Trust Levels and Timing Scenarios.

As discussed, the CASHMA scheme evaluated based on a session timeout mechanism; this approach also incubates the trust levels for a service and third party service provider. The trust level is directly imposed on data transferred and the speed of service reliability. In general time of a session t_s should always be less than deemed time for data session under an untrusted web service network.

IV. DISCUSSION

In CASHMA scheme, a valid biometric system is been used (Fingerprint) and thus we can state an enhancement for continues and secure data serving on an untrusted domain. In our future contribution, a dedicated OTP (One time Password) system can be used and in-cooperated for a continues timeout

authentication on a reliable note.

Generally, under a single user handling services such as e-commerce and banking, a biometric authentication system become complicated and complex under various scenarios. Thus as proposed an enhancement OTP system can reduce the overall cost model and also can be user-reachability. As the CASHMA bio-metric system has a thread model causes and thus the performance of scheme is reduced. This performance threads are focused towards the data exchange bit rates and hence from the enhancement, a complete bit transfer is been avoided from the sender end.

V. CONCLUSION

CASHMA protocol is a certified and a reliable internet scheme with add-on monitoring schemes such as Scenario measurement, ADVICE enhancement and Trust level determination. Apparently, we have also seen a Bio-Metric verification for continues authentication under a session. This impacts the performance ratio of the system and hence an enhancement of OTP is suggested with a concept of implementation.

REFERENCES

1. Ojala, S., Keinanen, J., & Skytta, J. (2008, November). Wearable authentication device for transparent login in nomadic applications environment. In *2008 2nd International Conference on Signals, Circuits and Systems* (pp. 1-6). IEEE.
2. Sim, T., Zhang, S., Janakiraman, R., & Kumar, S. (2007). Continuous verification using multimodal biometrics. *IEEE transactions on pattern analysis and machine intelligence*, *29*(4), 687-700.
3. Montecchi, L., Lollini, P., Bondavalli, A., & Mattina, E. L. (2012, September). Quantitative security evaluation of a multi-biometric authentication system. In *International Conference on Computer Safety, Reliability, and Security* (pp. 209-221). Springer, Berlin, Heidelberg.
4. Li, S. Z., & Jain, A. (2015). *Encyclopedia of biometrics*. Springer Publishing Company, Incorporated.
5. LeMay, E., Unkenholz, W., Parks, D., Muehrcke, C., Keefe, K., & Sanders, W. H. (2010, September). Adversary-driven state-based system security evaluation. In *Proceedings of the 6th International Workshop on Security Measurements and Metrics* (pp. 1-9).
6. Courtney, T., Gaonkar, S., Keefe, K., Rozier, E. W., & Sanders, W. H. (2009, June). Möbius 2.3: An extensible tool for dependability, security, and performance evaluation of large and complex system models. In *2009 IEEE/IFIP International Conference on Dependable Systems & Networks* (pp. 353-358). IEEE.
7. Ahmed, S. T. (2017, June). A study on multi objective optimal clustering techniques for medical datasets. In *2017 international conference on intelligent computing and control systems (ICICCS)* (pp. 174-177). IEEE.
8. Nicol, D. M., Sanders, W. H., & Trivedi, K. S. (2004). Model-based evaluation: from dependability to security. *IEEE Transactions on dependable and secure computing*, *1*(1), 48-65.
9. Singh, K. D., & Ahmed, S. T. (2020, July). Systematic Linear Word String Recognition and Evaluation Technique. In *2020 International Conference on Communication and Signal Processing (ICCSP)* (pp. 0545-0548). IEEE.
10. Sheyner, O., Haines, J., Jha, S., Lippmann, R., & Wing, J. M. (2002, May). Automated generation and analysis of attack graphs. In *Proceedings 2002 IEEE Symposium on Security and Privacy* (pp. 273-284). IEEE.